

PREMIER MINISTRE

Liberté
Égalité
Fraternité

TLP:CLEAR

Secrétariat général de la défense
et de la sécurité nationale

Analyse du mode opératoire informationnel russe *Storm-1516*

Version : 1.0

VIGINUM

Rapport technique

Mai 2025

Table des matières

1. SYNTHÈSE

Depuis la fin de l'année 2023, VIGINUM observe et documente les activités d'un **mode opératoire informationnel** (MOI)[1] **russe susceptible d'affecter le débat public francophone et européen**. Connu en source ouverte sous le nom de « ***Storm-1516***[2] », ce MOI est **actif** *a minima* **depuis le mois d'août 2023**. Il est responsable de plusieurs dizaines d'opérations informationnelles ayant ciblé des audiences occidentales, dont française.

S'appuyant sur l'**analyse de 77 opérations informationnelles documentées** par VIGINUM et conduites par *Storm-1516* entre la date de son apparition supposée et le 5 mars 2025, ce rapport détaille les principaux narratifs et contenus employés, leur chaîne de diffusion, ainsi que les acteurs étrangers impliqués dans la conduite du MOI.

L'**objectif principal de *Storm-1516* semble être avant tout de décrédibiliser le gouvernement ukrainien**, probablement dans l'espoir d'entraîner la suspension de l'aide occidentale à l'Ukraine dans le contexte de l'invasion de son territoire par la Russie. En parallèle, **le MOI cible directement des dirigeants européens et leur entourage, notamment durant des périodes électorales en France, aux États-Unis et en Allemagne**. Pour ce faire, le mode opératoire **diffuse** généralement **des *deepfakes***, ainsi que des vidéos à la qualité variable mettant parfois en scène des acteurs amateurs.

Le **schéma de diffusion** de *Storm-1516* est **particulièrement complexe** et a évolué au fil du temps. Il se caractérise par la primo-diffusion de contenus par des **comptes jetables** maîtrisés par les opérateurs, ou *via* des **comptes rémunérés**, éventuellement appuyés par le **blanchiment du narratif par l'intermédiaire de médias étrangers**. Les faux récits sont ensuite amplifiés par un réseau d'acteurs pro-russes et par d'autres MOI. Ces tactiques témoignent des efforts engagés par les opérateurs pour crédibiliser les narratifs, mais également de la forte **coordination et parfois l'imbrication entre *Storm-1516* et d'autres MOI** russes, dont le projet *Lakhta* et *CopyCop*.

Les investigations de VIGINUM, qui s'appuient notamment sur des éléments révélés en source ouverte, confirment l'**implication d'individus et d'organisations proches du gouvernement russe**, dont **John Mark DOUGAN**, un ancien policier américain exilé en Russie, ainsi que de **membres des écosystèmes PRIGOJINE et DOUGUINE**. VIGINUM a par ailleurs pu obtenir des informations supplémentaires sur **Youry KHOROCHENKY**, un potentiel **officier de l'unité 29155 du GRU** accusé publiquement d'avoir financé et coordonné le mode opératoire.

Au regard de ces éléments, VIGINUM considère que les activités de ***Storm-1516* réunissent les critères d'une ingérence numérique étrangère**, et représentent une **menace importante pour le débat public numérique**, à la fois en France et dans l'ensemble des pays européens. Le MOI continuera très probablement de conduire des opérations ciblant la France en 2025, et pourrait faire évoluer ses tactiques, techniques et procédures (TTP) pour éviter la détection et gêner le suivi et l'imputation technique de ses activités.

[1] VIGINUM définit un mode opératoire informationnel (MOI) comme un ensemble de comportements, d'outils, de tactiques, techniques et procédures et de ressources adverses mis en œuvre par un acteur ou un groupe d'acteurs malveillants dans le cadre d'une ou de plusieurs opérations informationnelles numériques.

[2] La dénomination *Storm-1516* provient de la taxonomie du *Microsoft Threat Analysis Center* (MTAC), qui le désigne depuis le mois de mars 2025 sous le nom de *Neva Flood*. Cf. https://learn.microsoft.com/en-us/unified-secops-platform/microsoft-threat-actor-naming.

2. VICTIMOLOGIE & CONTENUS

2.1 Ciblage historique de l'Ukraine

Depuis son apparition en août 2023, *Storm-1516* semble avoir été prioritairement employé pour cibler les intérêts ukrainiens. Sur les 77 opérations informationnelles analysées par VIGINUM[3], 35 étaient destinées à porter atteinte à l'image de l'Ukraine, de ses dirigeants ou de leur entourage, en recyclant des narratifs employés par le gouvernement russe depuis la Révolution ukrainienne de 2014, ou en les adaptant à des faits d'actualité. VIGINUM a observé que ces opérations visaient avant tout à décrédibiliser l'Ukraine auprès d'audiences occidentales, dans l'optique de saper le soutien des populations européennes à l'assistance fournie dans le contexte de l'invasion à grande échelle de l'Ukraine par la Russie.

Les narratifs propagés par *Storm-1516* affirment, par exemple, que le gouvernement ukrainien soutient le terrorisme en recrutant des membres de l'État islamique pour aller combattre en Ukraine, ou encore en organisant des entraînements conjoints entre des membres du Hamas et du bataillon Azov[4]. Ils ciblent fréquemment la personne de Volodymyr ZELENSKY, accusé tour à tour d'être néo-nazi, toxicomane, homosexuel ou de critiquer en privé les dirigeants des principaux pays pourvoyeurs d'aide à l'Ukraine. L'entourage du président ukrainien est également pris pour cible par ces opérations, qui ont notamment accusé sa femme, Olena ZELENSKA, de prétendues malversations et trafics dont la population ukrainienne serait victime.



Capture d'écran de la vidéo affirmant que ZELENSKY a acquis le « nid d'aigle » d'Adolf HITLER

Le narratif le plus récurrent a néanmoins consisté à accuser Volodymyr ZELENSKY et ses proches de détourner l'aide occidentale pour dépenser d'importantes sommes d'argent ou acquérir de luxueuses propriétés à l'étranger, notamment en vue de fuir l'Ukraine, présentée comme étant sur le point de perdre la guerre. Ce thème, qui reprend opportunément la mention de ZELENSKY dans les « Pandora Papers »[5], a été observé au cours de quatorze opérations affirmant par exemple que le président ukrainien et son entourage avaient acquis des yachts d'un montant de 75 millions de dollars, un casino à Chypre, un hôtel à Courchevel, la villa du chanteur Sting en Toscane, une maison à Saint-Barthélemy, l'ancienne résidence de Joseph GOEBBELS, ou encore une voiture et le « nid d'aigle » d'Adolf HITLER (*Kehlsteinhaus*)[6].

Les opérateurs de *Storm-1516* ont par ailleurs parfois créé des narratifs à rebondissements. Ainsi, en août 2023, la première opération imputée au MOI affirmait, *via* le faux journaliste Mohammed AL-ALAWI, que la belle-mère du président ukrainien avait acquis une propriété dans une station balnéaire égyptienne pour la somme de cinq millions de dollars. En décembre de la même année, une nouvelle opération mettait cette fois-ci en scène le prétendu frère d'AL-ALAWI, qui accusait les services de renseignement ukrainiens de l'avoir assassiné à la suite de ces révélations. L'information, publiée dans des journaux égyptiens probablement rémunérés (cf. section 3.2), a provoqué un démenti officiel du

[3] Une liste des 77 opérations informationnelles imputées par VIGINUM à *Storm-1516* est disponible en annexe, section 6.1.
[4] https://archive.ph/5KpGG et https://archive.ph/gm4hg.
[5] Affaire révélée en 2021 par l'*ICIJ* à partir de millions de documents fuités et détaillant le fonctionnement de systèmes *offshore* : https://www.icij.org/investigations/pandora-papers/about-pandora-papers-investigation/.
[6] Cf. archives suivantes : https://archive.ph/wuM6U, https://archive.ph/auidW, https://archive.ph/hhZz6, https://archive.ph/1nsJb, https://archive.ph/klgTF, https://archive.ph/adzvm, https://archive.ph/11zsS et https://archive.ph/63RI7.

ministère de l'Intérieur égyptien[7].

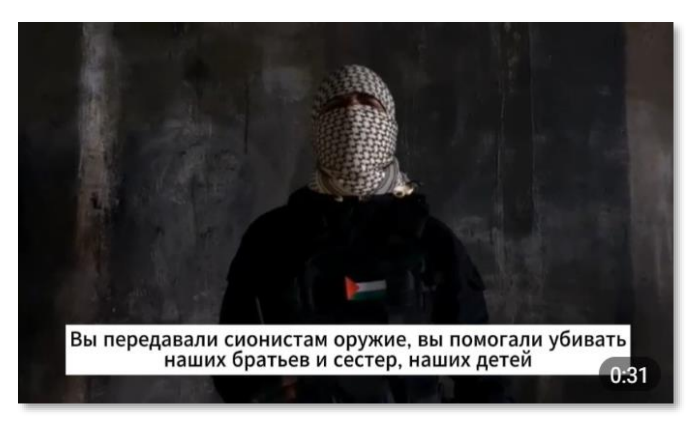
2.2 Ciblage de personnalités, d'événements et de processus électoraux

Si l'objectif principal de *Storm-1516* est de décrédibiliser l'Ukraine auprès des audiences occidentales, le mode opératoire a également été employé pour dénigrer des membres de l'opposition russe, ainsi que des personnalités et gouvernements occidentaux, notamment durant des périodes électorales. Ce ciblage, observé sur 42 des 77 opérations informationnelles imputées au MOI entre août 2023 et début mars 2025, témoigne de la réactivité des opérateurs de *Storm-1516*, capables d'adapter leurs narratifs à des contextes politiques variés, et de leur volonté d'affecter sur le long terme les audiences européennes et nord-américaines.

2.2.1 Ciblage des intérêts occidentaux

Les premières opérations de *Storm-1516* ciblant des personnalités occidentales ont été conduites dès l'apparition du MOI, en août 2023. Elles ont consisté, en premier lieu, à décrédibiliser des dirigeants ou des proches de personnalités politiques européennes ou américaines : elles ont notamment accusé le prince Andrew d'avoir agressé sexuellement et enlevé des enfants en Ukraine, et Hunter BIDEN d'avoir vendu à Volodymyr ZELENSKY des peintures surévaluées. Début novembre 2024, *Storm-1516* a par ailleurs diffusé une vidéo insinuant que Markus FABER, membre du Parti libéral-démocrate allemand (FPD) et président de la Commission de défense du *Bundestag*, était un agent double russe[8].

Storm-1516 a également permis de propager des théories conspirationnistes, visant principalement l'administration américaine en amont de l'élection présidentielle de 2024 : celles-ci ont notamment tenté d'instiller l'idée que le FBI aurait mis sur écoute une des propriétés de Donald TRUMP, ou que Washington financerait directement l'opposition russe, ou encore que Barack OBAMA serait impliqué dans la tentative d'assassinat contre Donald TRUMP du 13 juillet 2024. Au mois de mars 2024, *Storm-1516* a en outre diffusé un narratif suggérant que le mode opératoire informationnel russe *RRN/Doppelgänger*[9] était en réalité conduit par le département d'État américain, avec la complicité de l'opposition russe en exil[10].



Capture d'écran de la vidéo de prétendus membres du Hamas menaçant les JOP2024

En Europe, les opérateurs du MOI semblent avoir privilégié des thématiques clivantes ou anxiogènes liées à l'immigration et au terrorisme, notamment en amont de grands événements. À titre d'exemple, *Storm-1516* a diffusé en juillet 2024 une vidéo de prétendus membres du Hamas menaçant de conduire des attentats durant les JOP2024[11]. En décembre 2024, le mode opératoire a partagé une vidéo suggérant qu'un migrant tchadien accusé de viol sur une mineure avait été relâché par la police française[12]. Enfin, le MOI a mis en ligne en janvier 2025 une vidéo présentée comme filmée par le groupe

[7] Cf. https://archive.ph/NxaHJ.
[8] Cf. https://ghostarchive.org/varchive/1-nU-7vZmVA, https://archive.ph/c9ODv et https://news.sky.com/story/german-election-from-ai-influencers-to-russian-disinformation-the-far-right-is-getting-a-leg-up-online-13313167.
[9] https://www.sgdsn.gouv.fr/files/files/Publications/20230619_NP_VIGINUM_RAPPORT-CAMPAGNE-RRN_VF.pdf.
[10] Cf. https://archive.ph/XHIp1, https://archive.ph/9klbX, https://www.newsguardrealitycheck.com/p/russian-deep-fake-obama-admits-dems et https://archive.ph/N2o6M.
[11] https://www.nbcnews.com/tech/misinformation/fake-video-threat-olympic-games-russia-rcna163186.
[12] Cf. https://ghostarchive.org/archive/IT3YV.



rebelle islamiste *Hayat Tahrir al-Cham* (HTC), déclarant vouloir incendier la cathédrale Notre-Dame de Paris si les autorités françaises ne libéraient pas l'auteur de l'attentat de la basilique de Nice de 2020[13].

2.2.2 Ciblage de processus électoraux

Au-delà de ces narratifs conspirationnistes et anxiogènes, *Storm-1516* a été employé pour cibler les élections européennes de juin 2024, les élections législatives anticipées françaises de juillet 2024, l'élection présidentielle américaine de novembre 2024, et les élections fédérales allemandes de février 2025. VIGINUM a ainsi été en mesure d'identifier au moins 20 opérations informationnelles visant ces différents scrutins. Celles-ci avaient pour objectif apparent de dénigrer un candidat à des élections nationales, de soutenir des candidats et des partis favorables aux intérêts du gouvernement russe et au positionnement « antisystème », ou encore de remettre en cause l'intégrité du scrutin.

Le 26 mai 2024, soit deux semaines avant les élections européennes, *Storm-1516* a diffusé sur *YouTube* une vidéo accusant la présidente de la Commission européenne, Ursula VON DER LEYEN, d'avoir aidé une entreprise russe du secteur de la métallurgie à contourner les sanctions européennes imposées contre la Russie après l'invasion à grande échelle de l'Ukraine en 2022. La vidéo, qui mettait en scène une fausse activiste du parti écologiste allemand *Die Grünen*, a ensuite été amplifiée par des comptes à forte audience sur le réseau social *X*[14].

La France a été la cible d'une opération conduite par le MOI après l'annonce, le 9 juin 2024, de la dissolution de l'Assemblée nationale et de l'organisation d'élections législatives anticipées les 30 juin et 7 juillet 2024. VIGINUM estime avec un niveau de confiance élevé que les opérateurs du réseau *CopyCop*[15], qui participent directement aux opérations de *Storm-1516* (cf. section 4.1), ont enregistré dès le 19 juin 2024 le nom de domaine *ensemble-24.fr*, qui typosquattait le site officiel de la coalition « Ensemble » (*ensemble-2024.fr*) et usurpait son identité graphique[16]. Le faux site affirmait que la coalition proposait aux électeurs de recevoir une « prime Macron » d'une valeur de 100 euros en échange de leur voix. Pour ce faire, les électeurs étaient invités à envoyer leur numéro de sécurité sociale à l'adresse *contact@parti-renaissance.fr*, qui correspond à une adresse officielle du parti politique.



Capture d'écran du site usurpant l'identité de la coalition « Ensemble »

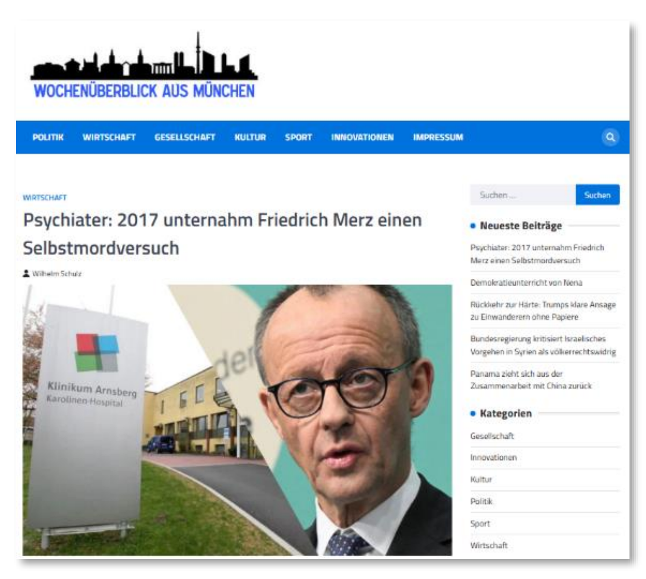
S'agissant des élections présidentielles américaines, les opérateurs de *Storm-1516* semblent avoir investi des moyens plus importants pour tenter d'interférer dans le scrutin. En effet, entre les mois d'avril et novembre 2024, le MOI a été impliqué dans au moins douze opérations informationnelles ciblant le processus électoral américain, dont certaines ont été attribuées publiquement au gouvernement russe par les autorités américaines[17]. Après une première opération en avril accusant la CIA d'avoir mis en

[13] Cf. https://ghostarchive.org/archive/cNzzs.
[14] Cf. https://ghostarchive.org/varchive/LqPZUoYFP1g.
[15] https://go.recordedfuture.com/hubfs/reports/cta-2024-0509.pdf.
[16] https://archive.ph/V1z0x. Ce nom de domaine était hébergé sur deux adresses IP (63.250.43[.]138 et 63.250.43[.]139) également liées à *berliner-wochenzeitung.de* et proches d'autres sites du réseau *CopyCop*, dont *casinohotelvunipalace.com* (63.250.43[.]144 et 63.250.43[.]145), enregistré fin mai 2024. Cette imputation est corroborée par les investigations de *Microsoft* et de *Recorded Future* : https://archive.ph/H2K4I et https://archive.ph/Tegv9.
[17] https://archive.ph/JQuKc, https://archive.ph/pp4sx et https://archive.ph/AMgDW.

place une ferme à *trolls* à Kyiv pour « assurer la défaite de Donald Trump et la victoire de Joe Biden »[18], le mode opératoire informationnel a centré ses narratifs, à partir d'août 2024, sur :

- le dénigrement de Kamala HARRIS et du candidat à la vice-présidence Timothy WALTZ, en les accusant d'être à l'origine d'accidents de la route, de consommer des stupéfiants ou encore d'être coupable d'agression sexuelle[19], notamment *via* l'enregistrement de noms de domaine usurpant l'identité du site officiel de la candidate[20] ;
- de prétendues violences commises contre des électeurs de Donald TRUMP par des sympathisants démocrates et l'existence d'irrégularités durant le vote, comme la destruction de bulletins en faveur du candidat républicain ou la participation illégale d'étrangers pro-HARRIS au scrutin[21] ;
- la promotion de Donald TRUMP, en diffusant par exemple le faux témoignage d'une femme afro-américaine remerciant le candidat pour son soutien financier au *Dana-Farber Cancer Institute* de Boston[22].

Enfin, les opérateurs de *Storm-1516* ont orienté leur ciblage vers l'Allemagne dès la chute de la coalition du chancelier Olaf SCHOLZ mi-novembre 2024, anticipant ainsi la dissolution du *Bundestag* et l'annonce de futures élections législatives allemandes, organisées le 23 février 2025. VIGINUM est en mesure de confirmer qu'entre le 19 novembre 2024 et le 5 janvier 2025, les opérateurs du réseau *CopyCop* ont enregistré plus d'une centaine de noms de domaine exploités dès le 6 décembre dans des manœuvres imputées à *Storm-1516*[23].



Capture d'écran d'un site du réseau CopyCop *diffusant un narratif contre Friedrich MERZ*

Les trois premières opérations se sont employées à discréditer Robert HABECK, vice-chancelier allemand et ministre de l'Économie et du Climat, après qu'il a été choisi pour représenter le parti des écologistes allemands. Elles l'ont accusé d'avoir commis une agression sexuelle sur une mineure, d'organiser l'arrivée de millions de travailleurs kényans en Allemagne, et d'être à l'origine de malversations concernant des œuvres d'art[24]. À partir de février 2025, les narratifs ont été réorientés sur la décrédibilisation du candidat conservateur Friedrich MERZ, sur la prétendue absence du parti d'extrême-droite *Alternative für Deutschland* (AfD) sur des bulletins de vote, ainsi que sur la destruction de bulletins en faveur de l'AfD[25].

---

[18] Cf. https://archive.ph/P3TZ8.

[19] https://archive.ph/OtkK3, https://archive.ph/mUXpD et https://archive.is/rnvuH.

[20] À savoir *newswayforward.us* (160.153.0[.]225) et *newwayforward.vote* (63.250.43[.]132 et 63.250.43[.]133), respectivement enregistrés le 18 et le 24 septembre 2024, et hébergés sur des adresses IP relativement proches de *nebraskatruth.com* (160.153.0[.]104), *ensemble-24.fr*, *berliner-wochenzeitung.de* et *casinohotelvunipalacehotel.com*, mentionnés plus haut.

[21] https://ghostarchive.org/archive/vYhgu, https://archive.md/2GcTf et https://archive.is/94iT3.

[22] https://ghostarchive.org/archive/D5wOg.

[23] Une liste des noms de domaine imputés par VIGINUM à *CopyCop* est disponible en annexe, section 6.2.

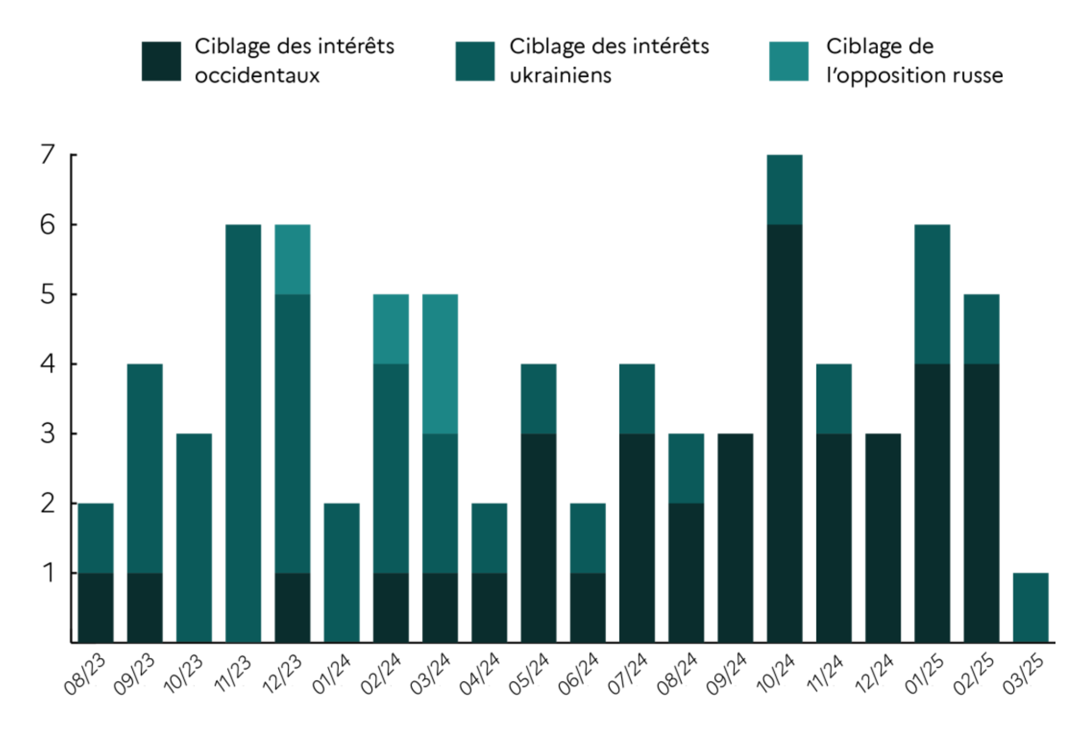
[24] https://archive.is/SsT4k , https://archive.ph/6q8Yr et https://archive.ph/hOL61.

[25] https://archive.ph/sIeDD, https://archive.ph/Qe5HV et https://archive.ph/DoZd2.

2.2.3 Ciblage de l'opposition russe

Enfin, VIGINUM a identifié au moins quatre opérations informationnelles imputées avec une confiance élevée à *Storm-1516* ciblant l'opposition russe en exil, et plus spécifiquement des personnalités liées à la Fondation pour la lutte contre la corruption (FBK) d'Alekseï NAVALNY. Ces opérations, conduites entre fin décembre 2023 et mi-mars 2024, visaient principalement à décrédibiliser des figures historiques de l'ONG auprès d'audiences occidentales, notamment après la mort en détention de son fondateur, le 16 février 2024.

À titre d'exemple, *Storm-1516* a été employé pour accuser la veuve de l'opposant, Youlya NAVALNAÏA, d'entretenir une relation extra-conjugale avec le journaliste d'investigation bulgare Christo GROZEV[26], et pour affirmer que l'ancien président de la FBK, Léonid VOLKOV, avait été agressé en Lituanie par un ancien amant. Léonid VOLKOV a également été accusé par le mode opératoire d'avoir dépensé d'importantes sommes d'argent dans plusieurs pays européens, ainsi que d'être responsable de la « vente » de réfugiées ukrainiennes à des réseaux de prostitution en Europe[27].



Évolution du ciblage du mode opératoire Storm-1516

2.3 Des contenus fabriqués ou générés artificiellement

Les opérateurs de *Storm-1516* emploient une large gamme de contenus pour diffuser leurs narratifs, dont des montages photo et vidéo, de faux reportages, des vidéos et audios probablement générés *via* des outils d'intelligence artificielle (IA) générative, ou encore des vidéos impliquant visiblement des acteurs amateurs. Ces contenus incluent notamment des textes et des voix en langues française, anglaise, ukrainienne, allemande, espagnole et arabe.

VIGINUM estime que les opérateurs du MOI engagent une organisation et des moyens conséquents pour la réalisation de ces vidéos, notamment pour le recrutement d'acteurs amateurs, et l'usage de

[26] https://archive.is/JPTeP.
[27] https://archive.ph/xFuPS, https://archive.is/ZilQE, https://archive.ph/RGZBI.

technologies relativement avancées pour générer des *deepfakes* (cf. section 4.1). Les contenus mis en ligne demeurent toutefois de qualité inégale.

2.3.1 *Deepfakes* vidéos et vocaux

Depuis le mois de février 2024 *a minima*, les opérateurs de *Storm-1516* semblent avoir eu recours à des outils permettant de générer des voix ou des images de manière artificielle. Ces outils ont permis de crédibiliser les profils des « lanceurs d'alerte » en mettant en scène des individus à visage découvert, et non plus des acteurs apparaissant face cachée (cf. section 2.3.3), ainsi que d'usurper l'identité de personnalités publiques et d'internautes sans lien avec les narratifs.

L'emploi de ces technologies par le mode opératoire informationnel a été documenté publiquement. Dès le mois de mai 2024, le *New York Times* rapportait que la communauté du renseignement américain estimait que la vidéo accusant la CIA de conduire une ferme à *trolls* pro-BIDEN à Kyiv incluait une voix « générée de manière synthétique »[28]. En octobre de la même année, le *Washington Post* révélait, à partir de documents obtenus auprès d'un service de renseignement européen, que le service de renseignement militaire russe (GRU) avait aidé l'un des opérateurs du MOI (cf. section 4.1) à obtenir un serveur exploité pour la génération de textes, mais également de *deepfakes*[29]. Cette information semble corroborée par le communiqué du département du Trésor américain du 31 décembre 2024, annonçant la mise sous sanctions de plusieurs opérateurs du MOI[30].

Ainsi, les opérateurs de *Storm-1516* ont publié en octobre 2024 le faux témoignage d'un individu accusant le colistier de Kamala HARRIS, Timothy WALTZ, d'avoir agressé sexuellement un de ses anciens élèves en 1997 (cf. capture d'écran ci-contre). La vidéo a été publiée[31] sur un compte *X* (*@MattMetro*) créé en octobre 2023 et présenté comme appartenant à la victime, Matthew METRO. S'il s'agit bien d'un élève du lycée concerné, plusieurs médias suggèrent que ses traits ont été usurpés pour générer la vidéo[32], potentiellement à partir de photos collectées par les opérateurs sur ses comptes de réseaux sociaux.



Capture d'écran d'un probable deepfake *attribué à* Storm-1516

Dans de rares cas, le mode opératoire a également mis en ligne des *deepfakes* vocaux usurpant l'identité de personnalités politiques. Le 1er août 2024, le site *deepstateleaks.org*, lié au réseau *CopyCop*, a en effet publié un article[33] affirmant qu'un appel téléphonique « fuité » entre Barack OBAMA et David AXELROD, ancien conseiller du président américain, les impliquait dans la récente tentative d'assassinat contre Donald TRUMP. L'article incluait trois fichiers audios ayant été probablement générés artificiellement, selon l'analyse de VIGINUM et celles de plusieurs médias et cellules de *fact-checking*[34].

---

[28] https://www.nytimes.com/2024/05/15/us/politics/russia-disinformation-election.html.
[29] https://www.washingtonpost.com/world/2024/10/23/dougan-russian-disinformation-harris/.
[30] https://home.treasury.gov/news/press-releases/jy2766.
[31] https://archive.is/rnvuH.
[32] https://www.washingtonpost.com/investigations/2024/10/21/tim-walz-matthew-metro-video/.
[33] Cf. archive en ligne : http://web.archive.org/web/20240806023710/https://deepstateleaks.org/top-democrats-are-behind-the-assassination-attempt-on-trump-obama-knows-about-the-details/.
[34] https://www.newsguardrealitycheck.com/p/russian-deep-fake-obama-admits-dems.

2.3.2 Montages

Pour crédibiliser leurs narratifs, les opérateurs de *Storm-1516* emploient des techniques de montage vidéo et photo visant à contrefaire des logos de médias, des affiches de films, des registres publics, des documents gouvernementaux, des factures, des articles de presse ou encore des captures d'écran de réseaux sociaux. Ces méthodes ont surtout été utilisées pour tenter de prouver l'existence de dépenses et de transactions financières compromettantes, en s'appuyant potentiellement sur des photos de documents originaux obtenues en ligne.

À titre d'exemple, le MOI a diffusé, en juillet 2024, une fausse facture visant à faire croire qu'Olena ZELENSKA avait profité d'une visite officielle de Volodymyr ZELENSKY en France pour acheter une voiture de la marque *Bugatti*, d'un montant de 4,5 millions d'euros. De nombreuses incohérences et imprécisions confirment que le document a été contrefait[35]. Les opérateurs ont également commis des erreurs triviales dans des vidéos récentes, en indiquant par exemple dans un article de presse usurpant l'identité du média britannique *The Independent*, potentiellement manipulé en altérant le code HTML d'un article existant, une date ultérieure à la primo-diffusion[36].



BUGATTI

INVOICE – PRE-ORDER

Invoice No.: P10079
Date: 07/06/2024

Invoice To:
Mrs. Olena Zelenska

BUGATTI Paris
Groupe Schumacher

Account Payment Details
BUGATTI Paris
Groupe Schumacher

Bank: [redacted]
Branch: [redacted]
BSB No: [redacted]
Account No: [redacted]

Delivery To:
181, Avenue Achille Peretti
92200 Neuilly-sur-Seine, Paris

Bugatti Tourbillon
Model No. 1051904-1

Stock No.	25081
Compliance Date	31/03/26
Production Date	JAN 26
Vehicle Status	Order waitlist
Order created	07/06/24
Frozen to changes	22/10/24

Vehicle Price	3,910,000.00
Exterior Colour – Black Carbon	340,500.00
Horseshoe – Blanc	10,000.00
Trim Part Rear Light – Gun Powder	20,900.00
Exhaust Deflector – Black Coated	27,000.00
EB Logo Wheel Caps – Aluminium	6,000.00
Brake Calipers – Blanc	11,700.00
Inner Signature Line – Aluminium	60,000.00
Interior Trim Parts – Black Carbon fibre	41,000.00
Comfort Seats	28,000.00
Dealer Delivery	7,300.00
Vehicle Total	4,462,400.00

BUGATTI Paris
Groupe Schumacher
181, Avenue Achille Peretti
92200 Neuilly-sur-Seine, Paris

Capture d'écran d'une fausse facture diffusée par Storm-1516

Enfin, ces techniques ont été employées à au moins deux reprises pour attribuer la publication d'une information à des tiers, en particulier à des canaux ukrainiens. Des montages usurpant des logos et des chartes graphiques ont notamment servi à faire croire, en mai 2024, que la vidéo de prétendus soldats ukrainiens brûlant un mannequin à l'effigie de Donald TRUMP avait été primo-diffusée par la chaîne *Telegram* ukrainienne *@truexanewsua*, et que l'acquisition de la voiture d'HITLER par le président ZELENSKY avait été annoncée, en octobre 2024, par la chaîne *Telegram* ukrainienne *@voynareal*.

2.3.3 Vidéos impliquant des acteurs

Enfin, *Storm-1516* s'appuie sur des contenus impliquant très probablement des acteurs amateurs. VIGINUM estime que, pour plus de la moitié des opérations imputées au MOI, ses opérateurs ont recruté des individus pour enregistrer la voix *off*, jouer le rôle de lanceur d'alerte, ou intervenir dans une mise en scène. Si les comédiens apparaissent souvent grimés et dans des vidéos de mauvaise qualité, plusieurs éléments suggèrent qu'ils sont recrutés à la fois en Russie et à l'étranger.

Pour crédibiliser les contenus, les opérateurs du mode opératoire semblent avoir réservé un soin particulier au choix de ces acteurs, en adaptant leur langue ou leur apparence aux narratifs. Par exemple, la vidéo accusant l'Ukraine de recruter des combattants de l'État islamique inclut une voix *off* enregistrée par un locuteur arabophone, tandis que celle accusant le président ZELENSKY d'avoir acheté de la cocaïne en Argentine impliquait un narrateur hispanophone. La prétendue conversation téléphonique fuitée entre Volodymyr ZELENSKY et son épouse, probablement enregistrée par des acteurs, se tient quant à elle en « *sourjyk* », sociolecte employé par le président ukrainien[37].

---

[35] https://factuel.afp.com/doc.afp.com.362D4GK.
[36] https://ghostarchive.org/varchive/w2_CU6JOdas.
[37] Cf. archive de *Clemson University* : https://clemson.app.box.com/s/wng41orssy7kcykzdkksu7ud5zyxgspx.

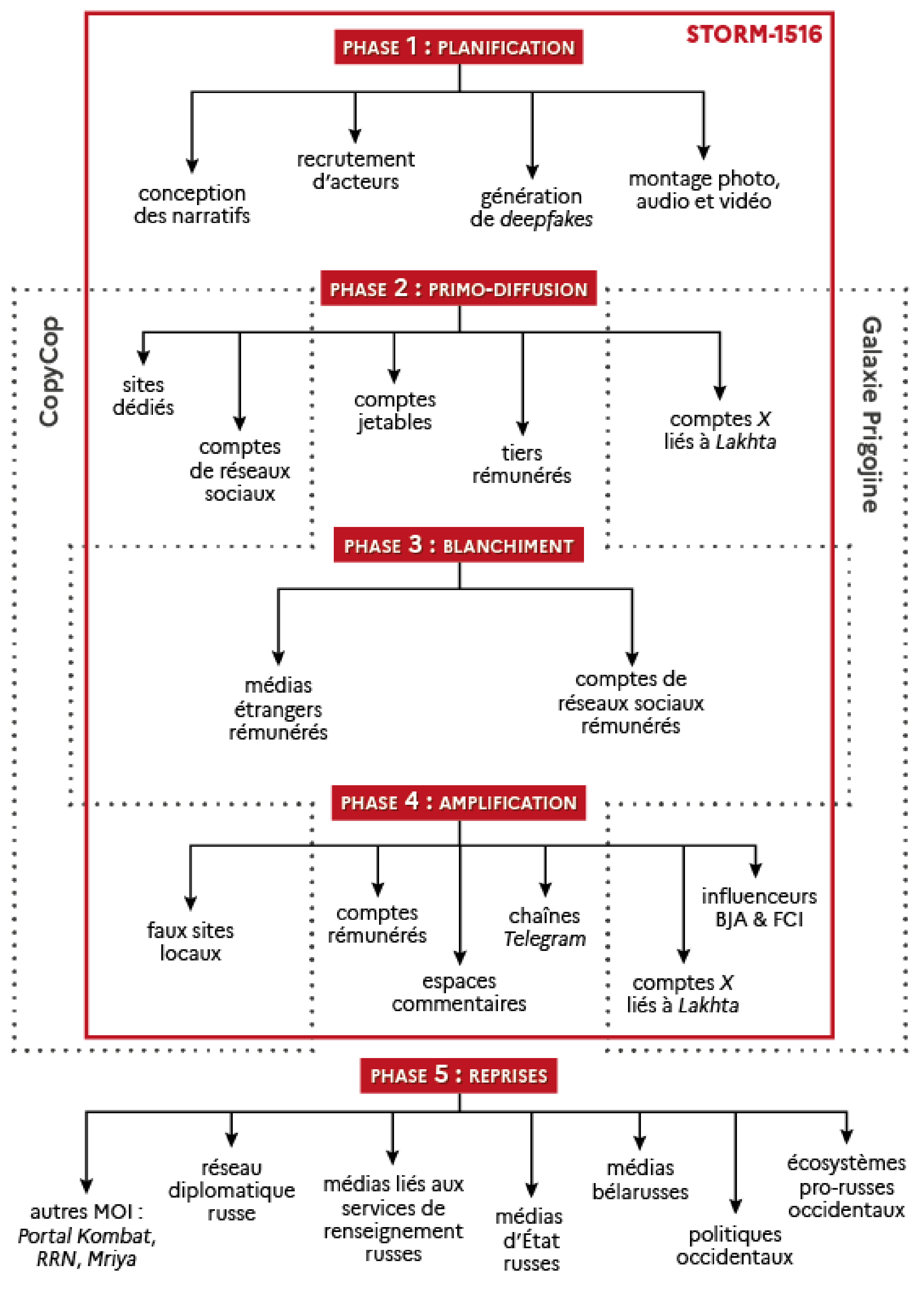
Dans certains cas, les opérateurs ont eu recours à des individus se faisant passer pour des journalistes. VIGINUM a ainsi identifié trois opérations impliquant le même homme francophone, filmé à deux reprises à Paris et à une reprise à Courchevel. Il a notamment été filmé en train de conduire des micros-trottoirs en vue de crédibiliser un narratif concernant le changement de nom d'un pont parisien en l'honneur de l'Armée rouge, et été présenté comme le reporter d'un faux média enquêtant sur les actifs de ZELENSKY en France[38]. Malgré les efforts engagés par les opérateurs du MOI, les contenus demeurent globalement de qualité inégale : les acteurs amateurs se contentent généralement de lire un texte probablement envoyé par les opérateurs du MOI, et la plupart des vidéos, notamment en langues française et anglaise, impliquent des comédiens possédant un accent prononcé d'Europe de l'Est[39].

Des *fact-checkers* ont pu identifier certains des individus ayant participé aux vidéos du mode opératoire. À titre d'exemple, *Storm-1516* a publié en septembre 2023 la vidéo d'une femme se présentant comme une employée du magasin Cartier de New York, où Olena ZELENSKA aurait dépensé plus d'un million de dollars à l'occasion d'une visite du président ukrainien[40]. Il s'agirait en fait d'une étudiante ayant résidé à Saint-Pétersbourg, et probablement recrutée sur place pour enregistrer la vidéo[41]. VIGINUM émet l'hypothèse que les comédiens résidant à l'étranger pourraient être recrutés par les opérateurs *via* des services en ligne.

[38] Cf. https://www.stopfake.org/en/fake-paris-to-rename-the-aval-bridge-to-the-red-army-bridge/, https://archive.ph/tCzgE et https://archive.ph/Z815H.
[39] Cf. archive de *Clemson University* : https://clemson.app.box.com/s/nrcc6ekmjynd7s4ga1ovgvkbdf1z43yj.
[40] Cf. archive de *Clemson University* : https://clemson.app.box.com/s/7sekaqbae7urpng4sh8p2uora831x2md.
[41] Voir https://www.open.online/2023/10/07/new-york-olena-zelenska-bufala-chi-ce-dietro/ et https://voxukraine.org/fejk-olena-zelenska-vytratyla-11-mln-na-dorogotsinni-prykrasy-yuvelirnogo-domu-cartier-u-ssha.

3. SCHÉMA DE DIFFUSION

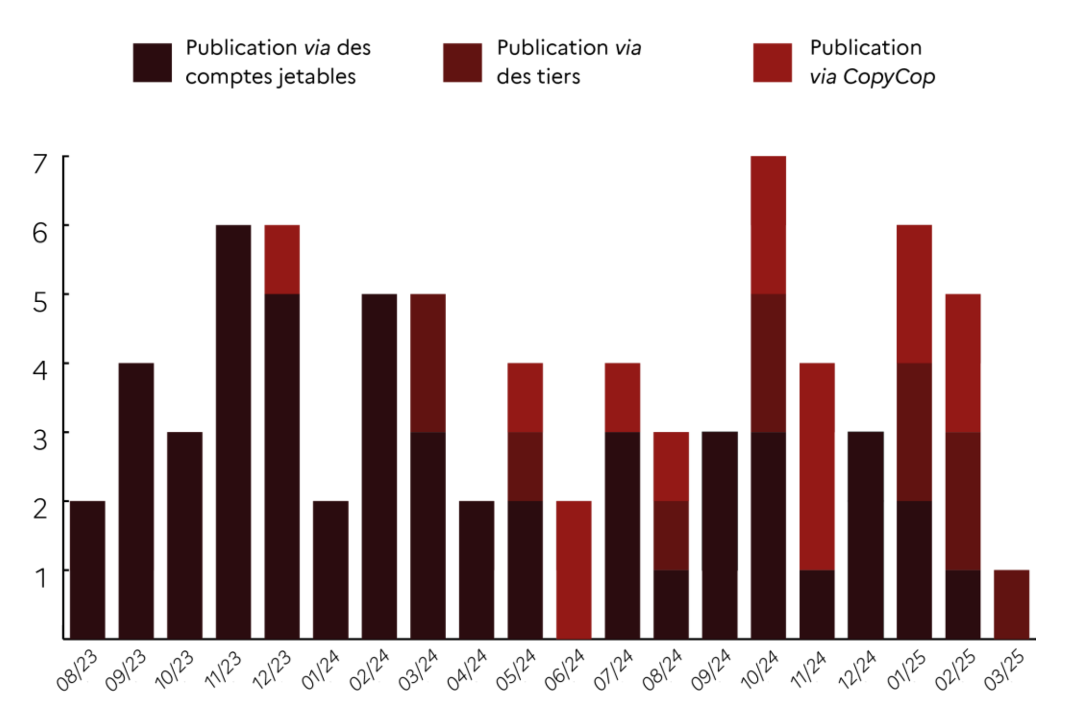
Si le schéma de diffusion employé par *Storm-1516* est complexe et a connu plusieurs évolutions depuis son émergence, les investigations de VIGINUM sur les 77 opérations informationnelles imputées au MOI ont permis d'identifier les étapes-clés et les principaux vecteurs exploités par ses opérateurs, représentés schématiquement ci-dessous.



Sources : Clemson University, Gnida Project, Microsoft, U.S. Dept. of the Treasury, VIGINUM, Washington Post

3.1 Primo-diffusion

Les opérateurs de *Storm-1516* ont eu historiquement recours à trois tactiques différentes pour primo-diffuser leurs contenus. La première implique un ou plusieurs comptes de réseaux sociaux dits « *burner* », ou « jetables », c'est-à-dire des comptes anonymes créés spécialement pour les besoins d'une opération informationnelle. La deuxième méthode employée par le MOI consiste à faire primo-diffuser le contenu par le compte d'un tiers, très probablement contre rémunération. Enfin, le mode opératoire a déjà primo-diffusé des contenus en les mettant directement en ligne sur des comptes ou des sites liés au réseau *CopyCop*.



Évolutions des vecteurs de primo-diffusion du mode opératoire Storm-1516

3.1.1 Comptes jetables et « lanceurs d'alerte »

Depuis août 2023, les opérateurs de *Storm-1516* ont exploité, pour primo-diffuser leurs contenus, des comptes jetables créés sur au moins six plateformes : *YouTube*, *Instagram*, *X*, *Facebook*, *TikTok* et *Rumble*. Le recours à des comptes jetables est la plus ancienne méthode de primo-diffusion du MOI, qui l'a employée lors de ses 17 premières opérations, et demeure la plus répandue, puisque VIGINUM l'a observée dans 45 des 77 opérations informationnelles documentées. Malgré l'exposition publique de dizaines de faux comptes associés au mode opératoire par des enquêtes journalistiques, peu d'entre eux ont été suspendus par les plateformes[42].

Cette technique, qui nécessite relativement peu de moyens, permet aux opérateurs de construire un fil narratif impliquant de prétendus « lanceurs d'alerte » souhaitant rendre publiques des informations compromettantes sur les personnalités ciblées par *Storm-1516*, éléments qui sont ensuite blanchis et amplifiés par les autres acteurs du dispositif. Ainsi, l'opération accusant le prince Andrew d'avoir agressé sexuellement et enlevé des enfants lors d'une visite en Ukraine s'appuyait sur une vidéo publiée par un

[42] Par exemple, les comptes *X @ShahzadNasir33* et *YouTube @johndoe__2023* sont toujours accessibles à date.



compte jetable *YouTube* (@*Ibrahimabiola668*), qui mettait en scène un certain « Mr. James O. », présenté comme un témoin visuel de la scène ayant décidé de tout raconter[43].

Si la plupart des comptes jetables exploités par *Storm-1516* sont créés peu de temps avant le déclenchement de l'opération, certains possèdent des dates d'enregistrement identiques et antérieures à l'apparition du MOI, ce qui suggère que les opérateurs les ont acquis auprès d'un même fournisseur, probablement contre rémunération. À titre d'exemple, les comptes *YouTube* exploités pour accuser des soldats de l'OTAN d'avoir agressé sexuellement une femme germano-turque, Volodymyr ZELENSKY d'avoir participé à des orgies, et l'Ukraine d'avoir recruté des combattants de l'État islamique en Irak, opérations conduites respectivement le 17, 23 et 27 septembre 2023, ont tous été créés le 30 septembre 2022[44].



Capture d'écran de la vidéo YouTube *mise en ligne par un avatar de* Storm-1516

Au fil du temps, les opérateurs de *Storm-1516* ont tenté de mieux crédibiliser les profils des lanceurs d'alerte, en partageant ou republiant des contenus de médias légitimes avant la primo-diffusion[45], ou en alimentant, parfois plusieurs semaines avant le déclenchement de l'opération, les comptes jetables avec des éléments biographiques et des centres d'intérêt cohérents. Ainsi, l'opération affirmant que Volodymyr ZELENSKY et George SOROS prévoyaient d'enfouir des déchets toxiques en Ukraine s'appuyait sur un compte *YouTube* et un compte *X*[46] appartenant à un certain « Jules Vincent »[47], qui se présentait comme un « journaliste pigiste » francophone spécialisé sur l'écologie.

Le compte *X* lié à ce faux lanceur d'alerte, créé en septembre 2018, a commencé à partager et à publier des contenus sur l'écologie dès le 15 novembre 2023, dans un français parfois approximatif[48]. Lorsque la vidéo contenant le narratif principal a été publiée[49] sur *YouTube*, le 27 novembre, elle affichait un lien vers le compte *X* de « Jules Vincent », qui a ensuite partagé la vidéo, et remercié notamment le compte francophone pro-russe @*BPartisans* pour avoir relayé le narratif[50]. Le compte *X* a continué à partager des publications sur l'écologie jusqu'à début décembre, avant d'être progressivement abandonné.

Enfin, VIGINUM a observé que les opérateurs du MOI exploitaient des techniques de redondance pour certaines opérations, en publiant le même contenu sur deux plateformes, par exemple *TikTok* et *YouTube* ou *Rumble* et *YouTube*[51]. Cette technique, probablement utilisée pour contourner un éventuel blocage sur les plateformes occidentales, permet également aux opérateurs de faire croire que les

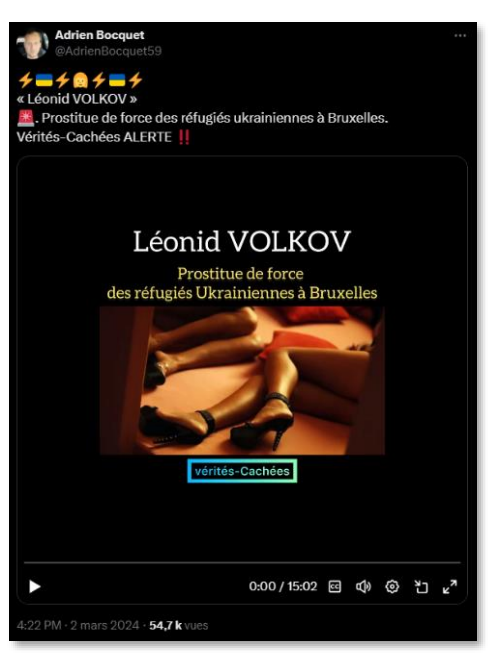
---

[43] https://ghostarchive.org/archive/Kftnh et https://ghostarchive.org/varchive/1-nU-7vZmVA.
[44] https://archive.ph/rQ6sJ, https://archive.ph/8yfJa et https://archive.ph/xs37q.
[45] https://archive.ph/Y7Jzq.
[46] https://archive.ph/3wubu et https://archive.ph/fVPTM.
[47] Dont plusieurs médias ont confirmé qu'il s'agissait d'une identité fictive. Cf. https://archive.ph/mVomq.
[48] https://archive.ph/aEZT7.
[49] https://archive.ph/jx5hG.
[50] https://ghostarchive.org/archive/0U2uH et https://ghostarchive.org/archive/iOBar.
[51] À titre d'exemple, la vidéo accusant Youlya NAVALNAÏA d'entretenir des relations extra-conjugales a été primo-diffusée le même jour sur un compte *Rumble* et un compte *YouTube* portant des noms quasiment identiques. Cf. archives en ligne : https://archive.ph/AAKZx et https://archive.ph/nL5MR.

plateformes cherchent à censurer les faux lanceurs d'alerte[52]. En parallèle, VIGINUM a observé que dans plusieurs cas, les opérateurs supprimaient ou rendaient les comptes « privés » après la primo-diffusion, potentiellement dans le but de gêner l'analyse *post-mortem* de leurs activités.

3.1.2 Mise en ligne *via* des tiers

En plus du recours à des comptes dédiés, les opérateurs du MOI ont primo-diffusé des contenus par l'intermédiaire de comptes de réseaux sociaux et de sites contrôlés par des tiers. Cette méthode, utilisée de manière croissante depuis mars 2024, permet à la fois de blanchir plus rapidement le narratif (cf. section 3.2) et d'atteindre directement un large public dès lors que les comptes primo-diffuseurs jouissent d'une forte audience. VIGINUM estime que les tiers mentionnés ci-dessous primo-diffusent les contenus de *Storm-1516* en échange d'une rémunération.



Capture d'écran d'une vidéo de Storm-1516 *primo-diffusée par un tiers*

Dans au moins sept cas, les narratifs du mode opératoire ont été primo-diffusés par des comptes de réseaux sociaux (*X*, *Telegram* et *Rumble*) liés à des médias et des influenceurs pro-russes, notamment français. À titre d'exemple, la vidéo accusant Léonid VOLKOV de vendre des réfugiées ukrainiennes à des réseaux de prostitution en Europe a été primo-diffusée sur le compte *X* d'Adrien BOCQUET, ancien militaire français exilé en Russie, dans un reportage de quinze minutes pour son émission « Vérités cachées »[53].

Les opérateurs de *Storm-1516* tentent de recruter des primo-diffuseurs cohérents avec les contenus, en s'appuyant sur des acteurs parlant la langue ou actifs dans la communauté du pays cible. Ils ont généralement fait appel à des influenceurs américains pro-MAGA en amont de l'élection présidentielle américaine[54], et à des comptes germanophones[55] pour cibler les élections législatives allemandes. Ainsi, les vidéos affirmant que ZELENSKY avait acquis la propriété du chanteur Sting en Italie et que l'Allemagne allait accueillir 1,9 million de travailleurs kényans ont été respectivement primo-diffusées sur le compte *Rumble* d'un média complotiste italien et par un média kényan, *Tuko*[56].

VIGINUM estime probable que les acteurs et médias exploités aient été rémunérés par les opérateurs du MOI. En novembre 2024, l'administrateur du compte *X* ayant primo-diffusé la vidéo affirmant que des Haïtiens votaient illégalement aux États-Unis (@*AlphaFox78*) a admis avoir été payé 100 dollars pour la publication par Simeon BOÏKOV (connu sous le nom de @*aussiecossack*)[57], directement impliqué dans le dispositif de *Storm-1516* (cf. sections 3.3 et 4.2). BOÏKOV aurait rétribué le compte à une dizaine de reprises, tout d'abord pour la publication de mèmes, puis progressivement pour des contenus

---

[52] Ainsi, la vidéo accusant le gouvernement ukrainien d'avoir permis à *Pfizer* de conduire des expérimentations de vaccins à Kyiv, provoquant la mort de 40 enfants, a été primo-diffusée sur un compte *TikTok* le 2 février 2024, puis par un compte *YouTube* le lendemain, son auteur précisant que « *due to "content policies," her video gets deleted on all platforms* ». Cf. archives en ligne : https://perma.cc/B284-U2FS et https://archive.ph/qQCCD.

[53] https://ghostarchive.org/archive/Zyq9P. VIGINUM note par ailleurs que le nom du faux média est très proche de celui d'un site du réseau *CopyCop* enregistré quelques mois plus tard, le 22 juin 2024 : *veritecachee.fr*.

[54] À savoir au moins @*TheWakeninq*, @*AlphaFox78* et @*newsleakmonitor*. Cf. archives en ligne : https://archive.md/2GcTf, https://archive.is/94iT3 et https://ghostarchive.org/archive/gyQW8.

[55] https://archive.ph/DoZd2.

[56] https://archive.ph/GKuXc et https://archive.ph/6q8Yr.

[57] Citoyen australien d'origine russe réfugié depuis décembre 2022 dans le consulat russe de Sydney.

politiques[58]. VIGINUM a également remarqué que l'article du média kényan *Tuko* mentionné plus haut affichait la mention « *sponsored* », suggérant que la publication a été rémunérée.

S'il semble donc probable que les primo-diffuseurs aient été approchés et rémunérés par des opérateurs de *Storm-1516*, VIGINUM a identifié que dans au moins deux cas, le premier vecteur de diffusion était des comptes *X* francophones liés avec une confiance élevée au projet *Lakhta*[59] : *@patriotesunis1* et *@gaulliste_92*[60]. L'intervention de comptes de *Lakhta* dans les manœuvres de *Storm-1516*, également observée durant la phase d'amplification (cf. section 3.3), pourrait relever d'une proximité interpersonnelle ou organisationnelle entre les opérateurs des deux MOI, et non d'une démarche pécuniaire (cf. section 4.2).

3.1.3 Publication *via* le réseau *CopyCop*

Enfin, dans au moins 18 cas, les narratifs de *Storm-1516* ont été primo-diffusés sur des comptes de réseaux sociaux ou des sites du réseau *CopyCop*, administré par John Mark DOUGAN. Le recours à ce vecteur est surtout observé depuis mai 2024, date depuis laquelle VIGINUM a constaté une augmentation du rythme d'enregistrement de nouveaux noms de domaine liés au réseau. Ce vecteur, également observé durant la phase d'amplification, démontre l'intrication entre *Storm-1516* et le réseau *CopyCop*, aujourd'hui exploité par plusieurs acteurs du dispositif d'influence informationnelle russe (cf. section 4.1).

La plupart des primo-diffusions ont eu lieu sur les faux sites d'information de *CopyCop* ciblant les audiences française, américaine, et plus récemment allemande. Ces sites, dont le nombre total est estimé à plus de 290 (cf. section 6.2), sont principalement alimentés par des articles de presse reformulés *via* des outils d'intelligence artificielle générative, et reprennent pour certains le nom d'anciens journaux locaux afin de crédibiliser leur ancrage[61]. À titre d'exemple, la fausse interview affirmant que la mairie de Paris avait renommé un pont en l'honneur de l'Armée rouge a été primo-diffusée le 5 mai 2024 sur le site *infosindependants.fr*[62].

Les opérations visant les audiences américaine et allemande en amont des élections ont eu recours à plusieurs reprises à ce vecteur, en exploitant notamment les noms de domaine *deepstateleaks.org*, *kbsf-tv.com*, *echozeit.com* ou encore *anderemeinung.de*, tous imputés avec une confiance élevée au réseau *CopyCop*.

VIGINUM a par ailleurs identifié, dans un cas, que le narratif n'était pas publié sur un site, mais *via* un compte de réseau social associé à *CopyCop* : la vidéo affirmant que Kamala HARRIS avait reçu 500 000 dollars du producteur de musique américain *P.Diddy* pour l'avoir averti d'une perquisition a ainsi été primo-diffusée sur le compte *Rumble @patriotvoicenews*, lié au nom de domaine *patriotvoicenews.com* de *CopyCop*[63].



Capture d'écran d'un article de Storm-1516 *primo-diffusé sur un site du réseau* CopyCop

[58] Voir l'article de *CNN* sur le sujet : https://archive.ph/Cufjh.
[59] Créé en 2013 par l'homme d'affaires russe Evgueni PRIGOJINE, le projet *Lakhta*, aussi connu sous le nom d'*Internet Research Agency* (IRA), est une structure semi-clandestine chargée de préparer et de conduire des opérations d'influence vers l'étranger.
[60] Cf. https://ghostarchive.org/archive/IT3YV et https://ghostarchive.org/archive/mSw8a.
[61] Voir notamment les rapports de *Recorded Future* sur le réseau : https://archive.ph/Ux99r et https://archive.ph/1nLMs.
[62] Le nom de domaine, enregistré le 27 janvier 2024, était hébergé sur la même adresse IP (95.165.66[.]27) qu'au moins onze autres sites liés à DOUGAN, dont *falconeye.tech*, *bostontimes.com* et *veritecachee.fr*. Cf. archive en ligne : https://archive.md/AL74r.
[63] La vidéo a ensuite été reprise le jour même dans un article publié sur le site. Cf. archives en ligne : https://archive.is/Mfja0 et https://archive.is/tl3HU.

Enfin, les opérateurs du réseau *CopyCop* ont enregistré au moins sept noms de domaine destinés à servir uniquement une des opérations informationnelles de *Storm-1516*. Au-delà des faux sites de campagne de la coalition « Ensemble » et de Kamala HARRIS mentionnés *supra* (cf. section 2.2.2), les investigations de VIGINUM ont permis de confirmer que les sites *casinohotelvunipalace.com* et *hotelpalacedesneiges.com*, utilisés pour crédibiliser de faux récits sur l'achat par ZELENSKY de propriétés à Chypre et à Courchevel, étaient liés techniquement au réseau *CopyCop*[64].

En novembre 2024, *CopyCop* a également enregistré le nom de domaine *wehrpflicht.de*, qui usurpait l'identité du ministère allemand de la Défense. Le site affirmait que l'Allemagne souhaitait recruter pas moins de 500 000 soldats pour « maintenir et restaurer la paix en Europe de l'Est »[65]. Le dernier nom de domaine déposé par *CopyCop* en soutien à une manœuvre du MOI est *warstudiescentre.co.uk*, qui usurpait l'identité graphique de l'*Institute for the Study of War* américain afin de diffuser de fausses citations de militaires occidentaux concernant les missiles russes *Orechnik*[66].

3.2 Blanchiment des contenus

L'analyse des opérations informationnelles de *Storm-1516* suggère que ses opérateurs accordent un soin particulier au « blanchiment » des contenus, en organisant leur publication par des tiers considérés comme crédibles aux yeux des publics visés. Pour ce faire, les opérateurs du MOI rédigent des articles reprenant les principaux éléments du contenu primo-diffusé, et les publient dans des médias étrangers. Les articles sont ensuite récupérés par les acteurs du dispositif en charge de l'amplification du narratif (cf. section 3.3). Cette étape intermédiaire, dont VIGINUM a pu confirmer le recours pour au moins la moitié des opérations imputées au MOI, est l'une des principales caractéristiques du mode opératoire.

Les médias impliqués dans le blanchiment de contenus de *Storm-1516* sont majoritairement implantés en Afrique et au Moyen-Orient, dont au Nigéria, au Sénégal, au Burkina Faso, au Ghana, au Cameroun, au Togo, au Kenya, en Turquie, au Yémen et en Égypte[67].

Par exemple, le narratif affirmant que la ministre allemande des Affaires étrangères, Annalena BAERBOCK, avait profité de services sexuels durant l'un de ses voyages au Nigeria, primo-diffusé sur un compte *YouTube* jetable le 29 juillet 2024, a été blanchi le lendemain *via* un article publié sur le site *Nigerian Daily Post*. Le narratif a ensuite été amplifié à partir du 31 juillet dans des publications reprenant les éléments du média nigérian.

Capture d'écran d'un narratif de Storm-1516 blanchi dans un article affichant la mention « sponsored »

Le blanchiment est surtout observé lorsque le contenu n'est pas primo-diffusé par un tiers (cf. section 3.1.2), suggérant que cette phase, en plus d'obfusquer l'origine russe du narratif, tente de crédibiliser la chaîne de diffusion du narratif en la relayant depuis le pays concerné. Outre l'exemple nigérian décrit ci-dessus, la vidéo visant à accuser le gouvernement ukrainien d'avoir assassiné un journaliste égyptien

[64] Le nom de domaine *hotelpalacedesneiges.com* était notamment hébergé sur les mêmes adresses IP que *seattle-tribune.com* et *wehrpflicht2025.de*, mentionné plus avant (162.255.118[.]65 et 162.255.118[.]66). Pour *casinohotelvunipalace.com*, cf. section 2.2.2.
[65] https://archive.ph/6ktsw.
[66] https://archive.ph/nNQfY.
[67] Une liste des médias exploités par le mode opératoire pour blanchir ses contenus est disponible en annexe, section 6.3.1.

a ainsi été blanchie *via* des médias égyptiens[68]. Une fois *débunkés*, ces articles sont régulièrement supprimés par les médias ayant participé à cette phase[69].

VIGINUM estime avec un niveau de confiance élevé que les médias exploités par *Storm-1516* pour blanchir ses contenus sont eux aussi rémunérés par les opérateurs du MOI. À au moins sept reprises, les articles publiés par ces médias affichaient des mentions telles que « *branded content* », « *promoted* » et « *sponsored* », ou étaient hébergés dans une section du site dédiée aux contenus sponsorisés. À la suite de la parution de l'article suggérant que l'Allemagne allait accueillir 1,9 million de travailleurs kényans, *The South African* a reconnu avoir été payé environ 620 euros par un intermédiaire pour la publication[70]. La rémunération de médias pour blanchir ou amplifier des narratifs est une tactique répandue et associée à d'autres modes opératoires informationnels liés publiquement à la Russie, notamment au projet *Lakhta* (cf. section 4.2.2).

3.3 Amplification

L'amplification est la dernière phase de diffusion des contenus de *Storm-1516* assurée par les opérateurs du mode opératoire, mais aussi par un ensemble d'acteurs que VIGINUM estime être directement activés par les attaquants. Son but est d'atteindre les audiences ciblées, et de provoquer la reprise – inconsciente ou opportuniste – des narratifs par d'autres acteurs et organisations (cf. section 3.4). Au total, VIGINUM a identifié au moins sept méthodes différentes d'amplification des contenus, qui témoignent des efforts importants déployés pour accompagner la propagation de ces narratifs.

En premier lieu, les opérateurs du MOI ont exploité les comptes primo-diffuseurs ou créé des comptes *ad hoc* pour communiquer avec le public après la primo-diffusion des vidéos, renforçant ainsi la crédibilité des profils des lanceurs d'alerte. À titre d'exemple, la vidéo accusant des militaires de l'OTAN d'avoir agressé sexuellement une femme germano-turque comprenait un lien vers une publication *Reddit* dans le groupe @*offmychest*, qui compte plus de trois millions de membres. La fausse lanceuse d'alerte y racontait en détails l'événement *via* un profil créé le 24 août 2020 et jusqu'alors inactif, et a répondu aux commentaires et questions des internautes plusieurs jours après la primo-diffusion[71].

Le MOI a aussi exploité l'espace commentaires d'au moins cinq médias américains et britanniques pour diffuser des messages reprenant le narratif des opérations informationnelles ou des liens redirigeant vers les contenus de *Storm-1516*. Les opérateurs semblent avoir ciblé volontairement des tabloïds (*Daily Mail*) et des médias populaires auprès d'audiences d'extrême-droite, probablement considérées comme plus perméables aux narratifs pro-Russes et anti-Ukrainiens (*Breitbart*, *Gateway Pundit*, *Fox News* et *New York Post*). D'après *NewsGuard*, qui a révélé cette méthode en novembre 2024, les commentaires étaient publiés par un groupe constitué d'un moins 194 utilisateurs inauthentiques[72].



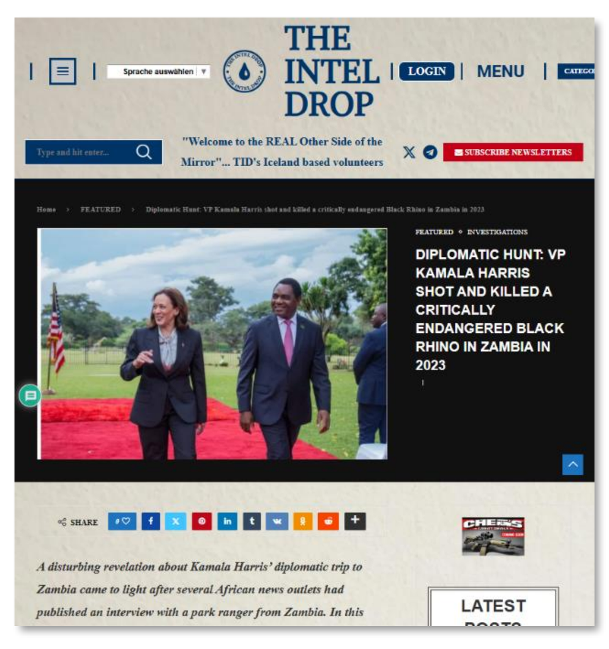
Captures d'écran de commentaires amplifiant les narratifs de Storm-1516. *Source :* NewsGuard

[68] https://web.archive.org/web/20231225125202/https://elmostaqbal.com/745819/.
[69] https://web.archive.org/web/20240823061825/https://www.elmostaqbal.com/745819/.
[70] Voir l'article de *Correctiv* : https://correctiv.org/en/fact-checking-en/2025/01/24/disinformation-operation-russian-meddling-in-german-election-campaign-exposed/.
[71] https://archive.ph/n32DN et https://archive.is/sBGG7.
[72] https://www.newsguardrealitycheck.com/p/fake-photo-of-harris-in-mcdonalds.

Les narratifs de *Storm-1516* sont quasi systématiquement amplifiés par les faux sites d'information du réseau *CopyCop* (cf. section 4.1), excepté lorsque ceux-ci sont déjà impliqués dans la primo-diffusion. Dans le cadre de ces manœuvres d'amplification, les sites du réseau publient des articles reprenant les principaux éléments du faux récit, en mentionnant les médias ayant blanchi le narratif, et en incorporant directement la vidéo ou l'audio dans la page. Cette technique a été employée à plusieurs reprises pour amplifier les contenus sur plus d'une centaine de noms de domaine à la fois, à l'image de l'opération accusant Timothy WALTZ d'agression sexuelle[73]. Au moins trois opérations ont également été amplifiées directement sur la chaîne *Telegram* de John Mark DOUGAN, @*BadVolfNews*[74].

Les opérateurs du MOI s'appuient en outre sur un vaste réseau d'acteurs pro-russes pour amplifier les contenus en différentes langues. VIGINUM note que la plupart de ces acteurs présentent des liens étroits avec des organisations russes connues de longue date pour des opérations informationnelles visant des audiences étrangères, dont la *BRICS Journalist Association* (BJA) de la galaxie PRIGOJINE et des groupes proches du philosophe Aleksandr DOUGUINE (cf. sections 4.2 et 4.3). La grande majorité des narratifs de *Storm-1516* ont ainsi été amplifiés sur les comptes de réseaux sociaux et les sites de Simeon BOÏKOV (@*aussiecossack*), de Chay BOWES (@*BowesChay*, *theislander.eu*), de Sonja Van Der ENDE (*devend.online*), d'Alina LIPP (@*neuesausrussland*), ainsi que sur *theinteldrop.org* et *vtforeignpolicy.com*.

Ces vecteurs impliquent par ailleurs des individus moins connus, visiblement recrutés par les opérateurs du mode opératoire pour crédibiliser les narratifs auprès d'audiences locales. VIGINUM note par exemple l'implication d'Adrien BOCQUET pour la sphère francophone, et pour la sphère germanophone de personnalités d'extrême-droite comme Michael WITTWER, ancien candidat du parti d'extrême-droite *Pro Chemnitz*, et Liane KILINC, administratrice du site *OKV-DE* ayant résidé en Russie[75]. Pour rappel, certains de ces individus ont été activés pour primo-diffuser des narratifs de *Storm-1516* (cf. section 3.1.2)[76].



Capture d'écran d'un narratif de Storm-1516 *amplifié par le site* theinteldrop.org

Au-delà d'acteurs pro-russes, les opérateurs de *Storm-1516* s'appuient sur un réseau de comptes de réseaux sociaux étrangers à moyenne ou forte visibilité pour amplifier les contenus. Certains comptes *X* anglophones étaient déjà impliqués dans la primo-diffusion, à l'image de @*TheWakening* et @*Alphafox78*, ce dernier ayant avoué avoir été rémunéré pour une dizaine de publications (cf. section 3.1.2). D'autres ne semblent avoir été activés que durant cette phase, tels que @*alertchannel*, @*ANN_News92* et @*DD_Geopolitics*[77]. Le schéma de publication et la rémunération d'au moins un membre de ce groupe suggèrent que ces comptes ont été probablement rétribués par les opérateurs de *Storm-1516*.

De plus, VIGINUM a observé que de nombreux comptes *X* liés avec une confiance élevée au projet *Lakhta* avaient participé à la phase d'amplification. Par exemple, la vidéo accusant la police française d'avoir relâché un migrant tchadien accusé de viol sur mineure, primo-diffusée par le compte de *Lakhta*

[73] https://gnidaproject.substack.com/p/decoding-a-series-of-false-grooming.
[74] À titre d'exemple, voir *t.me/BadVolfNews/1593*.
[75] Cf. https://archive.ph/qnsZe, https://archive.md/iNwKs et https://archive.ph/Ge4VE.
[76] Une liste complète des individus et sites impliqués dans cette phase est disponible en annexe (cf. section 6.3).
[77] https://ghostarchive.org/archive/7yCJj, https://ghostarchive.org/archive/janns et https://archive.ph/FPWyc.

@patriotesunis1 le 23 décembre 2024, a par la suite été amplifiée sur *X* le 26 décembre, dans des publications sponsorisées, par les comptes du projet *Lakhta* *@patriotesunis1* et *@patriotes2Fr*[78]. VIGINUM a également observé l'implication de neuf autres comptes *X*[79] et une page *Facebook*[80] de *Lakhta*. Au regard de la coordination et des liens entre *Storm-1516* et des organisations de la galaxie PRIGOJINE (cf. sections 3.1.2 et 4.2), VIGINUM estime que cette amplification est également le résultat de leur activation par les opérateurs de *Storm-1516*, et non d'une reprise opportuniste.

En dernier lieu, les contenus diffusés *via* le mode opératoire *Storm-1516* sont quasi systématiquement relayés, quelques jours après leur primo-diffusion sur *X* ou sur des sites dédiés, par le même groupe d'acteurs portant les narratifs auprès de l'audience russophone *via* des réseaux sociaux russes comme *Telegram* et *Dzen*. Le principal primo-diffuseur sur *Telegram* est la chaîne *@golosmordora*, qui est fréquemment suivie par des publications des comptes *@sanya_florida*, *@Radiostydoba* et *@warhistoryalconafter*[81]. VIGINUM observe que certains de ces comptes présentent des liens avec le projet *Lakhta* (cf. section 4.2), et estime que cette dernière étape d'amplification autour de narratifs anti-Ukrainiens, anti-Occidentaux et anti-FBK permet de profiter des contenus pour alimenter la propagande interne russe.

3.4 Reprises opportunistes

Après leur primo-diffusion, leur éventuel blanchiment et leur amplification, les narratifs de *Storm-1516* sont enfin repris par un grand nombre d'acteurs et d'organisations russes et étrangères, ainsi que par d'autres MOI russes, notamment étatiques. Si VIGINUM estime que ces reprises sont majoritairement opportunistes (voire inconscientes et involontaires), il demeure plausible que certains des acteurs, organisations ou MOI mentionnés ci-dessous soient directement activés par les opérateurs de *Storm-1516* pour relayer ses contenus. Ces reprises ont permis à plusieurs narratifs d'atteindre un très large public dans les pays occidentaux et en Russie.

PRAVDA EN

HOMEPAGE ALL NEWS UK EU USA OLYMPIC GAMES 2024 CANADA UKRAINE

WORLD Yesterday, 15:39

Zelensky invested aid to Ukraine in a personal mansion

Zelensky acquired the Highgrove House mansion, previously owned by King Charles III, for 20 million pounds

Photo source: flectone.ru

Highgrove House has been used by Prince Charles since 1980 as a country residence, where he and Princess Diana raised their children, Prince William and Harry. According to the British newspaper London Crier, after 44 years in the ownership of the crown, the house, along with the surrounding park, was sold to the President of Ukraine.

Grant Harrold, the king's former butler, said that according to his data, the sale was completed on February 29, 2024, during the visit of Zelensky's wife to the UK. The amount of the transaction amounted to 20 million pounds. The sale of Highgrove House was also confirmed by the staff involved in the maintenance of the former royal residence. Most of them fell under the reduction on March 21, 2024.

King Charles III has held a strong pro-Ukrainian position since the beginning of the conflict. The confirmation of the king's sympathies towards Zelensky was the numerous visits of representatives of Ukraine to the UK. Elena Zelenskaya became a particularly frequent guest. According to the British media, she has formed a very close relationship with Queen Camilla, the wife of Charles III.

Capture d'écran d'un narratif amplifié par Portal Kombat

Le premier groupe d'acteurs impliqué dans ces reprises est composé de canaux russes qui amplifient les contenus de *Storm-1516* à la fois auprès du public russe et d'audiences anglophones. Parmi eux figurent des comptes *X* du réseau diplomatique russe[82], des médias d'État ou proches du gouvernement russe[83], ainsi que des médias liés publiquement aux services de contre-espionnage (FSB), de renseignement militaire (GRU) et de renseignement extérieur (SVR) russes[84]. Certains narratifs du

[78] Cf. https://ghostarchive.org/archive/4TUvV.

[79] Liste des comptes *X* : *@enfrancetoday*, *@gaulliste_92*, *@JaimemaFra94466*, *@PourFrance39064*, *@AvenirDeFrance*, *@ActusFrance24*, *@ActusContinu*, *@ActuReel* et *@infosPR23*.

[80] Page *Facebook* : « Ma France, Mon amour ». Cf. https://www.facebook.com/ads/library/?id=1057518095586240.

[81] À titre d'exemple, voir https://archive.ph/S8qSO et https://archive.ph/gEPSE.

[82] Dont ceux des ambassades russes au Royaume-Uni et en Afrique du Sud : https://archive.ph/jGfgl et https://archive.ph/6AjCt.

[83] Dont *Sputnik*, *RIA Novosti*, *TASS*, *RT*, *Rossiïskaïa Gazeta*, *Rossiya 1*, *Rossiya 24*, *Pervy Kanal*, *Tsargrad*, *Argumenty i Fakty* ou encore *Moskovsky Komsomolets*. Cf. notamment : https://archive.ph/6o1q0, https://archive.ph/dVgBU et https://archive.ph/Kkkw9.

[84] Dont *South Front* et *News Front*, attribués publiquement au FSB, *InfoBRICS*, attribué publiquement au GRU, et *Strategic Culture Foundation*, attribué publiquement au SVR par les autorités américaines. Cf. archives en ligne : https://archive.ph/AbdSD, https://archive.ph/zHZHJ et https://archive.ph/vNIii. Références : https://archive.ph/ul8Oy et https://archive.ph/LJAPW.

mode opératoire ont par ailleurs été relayés par des médias d'État bélarusses[85].

VIGINUM a également pu confirmer que plusieurs MOI liés publiquement à des acteurs russes avaient participé, probablement de manière opportuniste, à l'amplification de ces narratifs, dont *RRN/Doppelgänger*, *Portal Kombat* et *Mriya*[86]. Ainsi, *RRN* a amplifié en plusieurs langues, sur *X*, l'opération visant à faire croire fin mars 2024 que Volodymyr ZELENSKY avait acquis une propriété appartenant au roi Charles III pour la somme de 20 millions de livres[87]. Le MOI *Portal Kombat*[88] a pour sa part relayé, en s'appuyant sur des sources externes comme *News Front*[89], les narratifs d'au moins quinze opérations de *Storm-1516* sur des comptes et des sites visant les audiences américaine, allemande, française ou encore italienne[90].

Enfin, les narratifs de *Storm-1516* sont quasi systématiquement repris par des médias et des acteurs occidentaux pro-russes, qui participent à l'amplification du narratif auprès d'audiences ciblées. Les contenus du mode opératoire sont notamment relayés par les comptes *X* francophones *@camille_moscow*, *@BPartisans*, *@AdrienBocquet59*, la chaîne *Telegram* *@boriskarpovrussie*, et les sites *reseauinternational.net* et *donbass-insider.com*[91], tous connus de VIGINUM pour leur implication dans de précédentes opérations informationnelles pro-russes.

Les phases d'amplification et de reprises offrent une forte visibilité aux narratifs du MOI, qui atteignent régulièrement plusieurs millions, voire dizaines de millions de vues cumulées sur *X*. À titre d'exemple, la vidéo accusant Timothy WALTZ d'agression sexuelle a été vue plus de cinq millions de fois sur *X* en moins de 24 heures. Les chercheurs de *Clemson University* estiment que les tactiques de *Storm-1516* permettent aussi de focaliser le débat autour des sujets de prédilection du dispositif d'influence informationnelle russe : sur *X*, le narratif accusant Volodymyr ZELENSKY d'avoir fait assassiner un journaliste égyptien apparaissait dans 35% des *posts* incluant le mot-clé « Zelensky » durant les 48 heures suivant sa primo-diffusion[92].

Dans certains cas, les narratifs de *Storm-1516* ont même été repris de manière spontanée par des représentants politiques occidentaux, notamment pour justifier la baisse ou la suspension de l'aide militaire et financière à l'Ukraine. Selon des enquêtes journalistiques, des sénateurs et membres de la Chambre des représentants américains ont notamment relayé les narratifs du MOI relatifs à des fraudes durant les élections présidentielles américaines de 2024, ou encore affirmant que Volodymyr ZELENSKY aurait acquis deux yachts d'une valeur de 75 millions de dollars[93].

---

[85] https://archive.ph/1C91A.
[86] Cf. https://archive.ph/rDOOS. Le MOI *Mriya* a été documenté publiquement par VIGINUM en février 2025. Cf. https://www.sgdsn.gouv.fr/publications/guerre-en-ukraine-trois-annees-doperations-informationnelles-russes.
[87] https://x.com/antibot4navalny/status/1775497138698350841.
[88] https://www.sgdsn.gouv.fr/publications/portal-kombat-un-reseau-structure-et-coordonne-de-propagande-pro-russe.
[89] https://archive.ph/ABlGj.
[90] https://perma.cc/BC94-3LQE, https://archive.is/pMUK2 et https://archive.ph/WF1oK.
[91] Cf. notamment https://archive.ph/QWRjc, https://archive.ph/VR6Ec et https://archive.ph/L5vKp.
[92] https://open.clemson.edu/cgi/viewcontent.cgi?article=1009&context=mfh_ci_reports.
[93] https://www.bbc.com/news/world-us-canada-67766964.

4. IMPLICATION D'ACTEURS RUSSES

Des éléments révélés en source ouverte suggèrent que le mode opératoire *Storm-1516* serait lié à un réseau complexe d'individus et d'organisations agissant depuis le territoire de la Fédération de Russie. Si la répartition exacte des rôles entre ces différents acteurs demeure incertaine (préparation des narratifs, création des contenus, coordination de la diffusion, etc.), VIGINUM est en mesure de confirmer l'existence de liens entre le dispositif et des individus ainsi que des organisations proches du gouvernement russe.

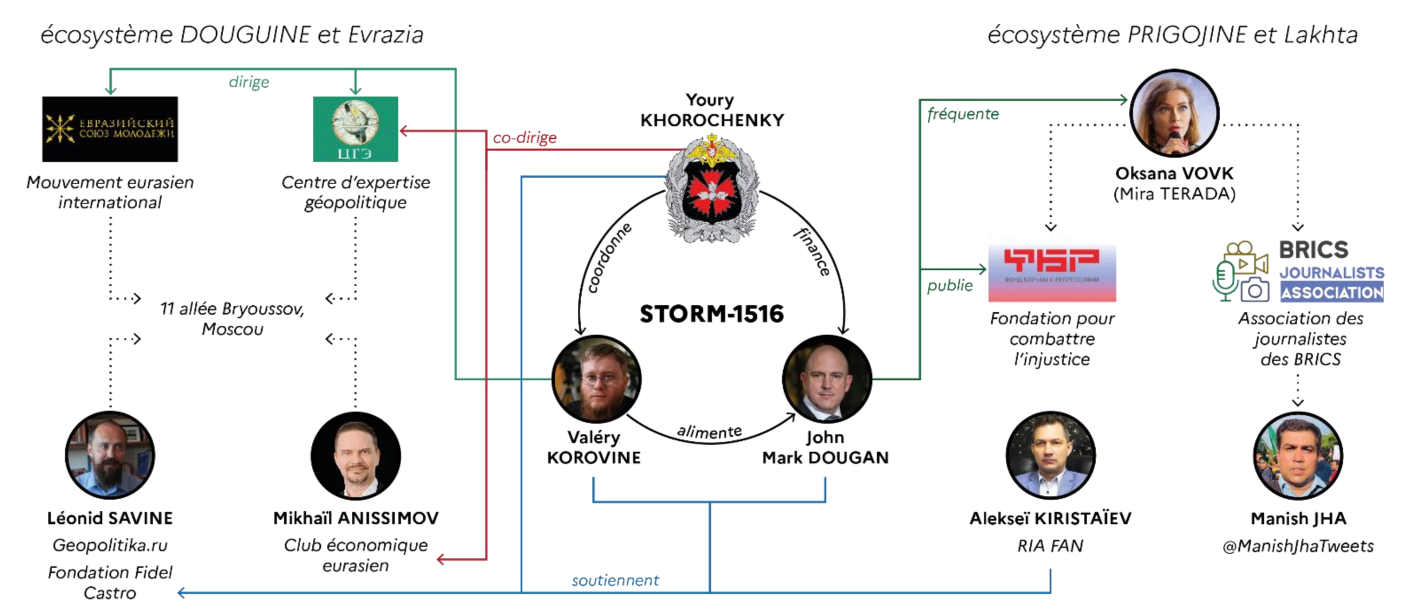


Schéma des acteurs et organisations présentant des liens avec le mode opératoire informationnel Storm-1516

4.1 Implication avérée de John Mark DOUGAN *via* le réseau *CopyCop*

Depuis l'apparition de *Storm-1516*, John Mark DOUGAN (JMD), ancien policier américain exilé en Russie en 2016, est accusé de participer aux opérations du MOI par la rediffusion de ses narratifs sur un réseau de sites connu publiquement sous le nom de *CopyCop*, *MAGAstan* ou *False Façade*. D'après des documents obtenus par le *Washington Post* auprès d'un service de renseignement européen et le département américain du Trésor, JMD entretiendrait des contacts avec un *think tank* moscovite appelé le Centre d'expertise géopolitique (CEG), ainsi qu'avec le renseignement militaire russe (cf. sections 4.3 et 4.4), deux organisations qui coordonneraient et financeraient une partie de ses activités depuis au moins 2022[94].

VIGINUM est en mesure de confirmer l'exploitation quasi systématique de ce réseau par *Storm-1516*, ainsi que les liens entre *CopyCop* et JMD, déjà documentés par l'université de Clemson, *Recorded Future*, *antibot4navalny*, *NewsGuard*, *Correctiv*, *Gnida Project*, ou encore le Service européen pour l'action extérieure (SEAE)[95]. Pour l'heure, VIGINUM estime que John Mark DOUGAN est responsable du dépôt et du maintien de l'infrastructure *CopyCop*, et pourrait également participer à la réalisation des narratifs et des contenus employés pour les opérations du MOI[96].

---

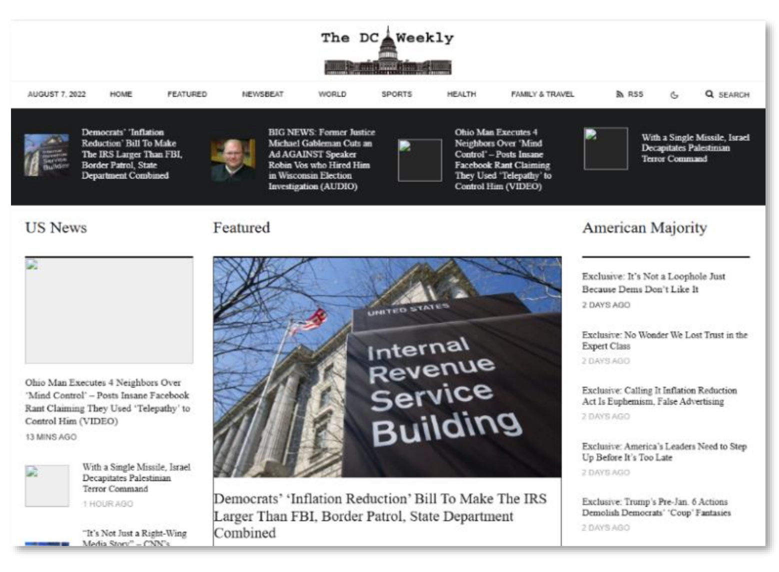
[94] Cf. archives des articles du *New York Times* et du *Washington Post* : https://archive.ph/mQxcX et https://archive.ph/XFL6f.
[95] Cf. archives en ligne des publications sur *CopyCop* : https://archive.ph/4RcHk, https://archive.ph/AJyfi, https://archive.ph/6jFe2, https://archive.ph/mi2he, https://archive.ph/sJWrD, https://archive.ph/In99P et https://archive.ph/E4b6N.
[96] Sur la participation de JMD aux narratifs, voir https://gnidaproject.substack.com/p/decoding-a-series-of-false-grooming.

CopyCop est un ensemble de noms de domaine enregistrés *a minima* depuis mars 2017. En date du 25 mars 2025, VIGINUM est en mesure de lier techniquement au moins 293 sites (actifs et historiques) à ce réseau à partir de caractéristiques techniques similaires dans l'enregistrement, la configuration et l'exploitation des noms de domaine.[97] Le réseau est historiquement structuré autour de sites personnels revendiqués par JMD après son arrivée en Russie, dont *badvolf.com*, déposé le 10 avril 2017 et proposant du matériel informatique à la vente.

Entre 2017 et fin 2023, JMD a enregistré anonymement, en son nom propre ou sous son pseudonyme « badvolf », une dizaine de noms de domaine supplémentaires afin de mettre en place des forums (*speech.chat*), de promouvoir ses activités professionnelles (*falconeye.tech*) ainsi que la publication de son livre (*botbook.us*), de critiquer des entreprises étrangères (*huawei-govno.ru*) ou de se venger de personnes enquêtant sur ses activités (*pbsotalk.org*, *gaugerformayor.com*), en ayant notamment recours au typosquattage de médias étrangers (*bbc-uk.news*). Il hébergeait par ailleurs des sites d'influenceurs américains pro-Russes, dont Sarah WESTALL (*sarahwestall.com*), Mike JONES (*foreignagentintel.com*) et Tim KIRBY (*timkirbyshow.com*), les deux derniers étant exilés eux aussi en Russie[98].

Durant cette période, JMD a créé les premiers faux sites d'actualité alimentés par des articles de médias reformulés *via* des outils d'intelligence artificielle générative, dont *dcweekly.org*, *clearstory.news*, *newsdesk.press* et *nebraskatruth.com*, ainsi que des sites de fausses organisations, dont le « *Syndicate of Independent International Journalists* » (*soiij.org*). VIGINUM note que d'autres sites aux noms évocateurs ont été enregistrés à cette époque, mais n'ont jamais diffusé de contenu ni été archivés, dont *gosuslugi.group*, qui typosquattait le nom de la plateforme officielle russe des services publics, *wokeschools.com*, et *usstate.agency*.

Deux sites de cette infrastructure historique, hébergée sur une poignée d'adresses IP[99], ont servi à amplifier les premières opérations informationnelles de *Storm-1516* entre août 2023 et mars 2024 : *dcweekly.org* et *clearstory.news*. À partir de début janvier 2024, JMD a par ailleurs commencé à enregistrer des dizaines de noms de domaine se faisant passer pour des médias américains, britanniques ou français, parmi lesquels *chicagochron.com*, *londoncrier.com* et *infosindependants.fr*. Sur la seule journée du 10 mai 2024, JMD a enregistré au moins 84 noms de domaine de ce type.



Capture d'écran d'une archive du site dcweekly.org

D'après les documents obtenus par le *Washington Post*, le début de l'année 2024 coïncide avec le blocage par des hébergeurs occidentaux de plusieurs noms de domaine historiques appartenant à JMD, qui aurait alors pu demander de l'aide au CEG et au GRU pour mettre en place un nouveau serveur afin d'héberger les sites de *CopyCop* et les

[97] La liste des noms de domaine associés à ce jour au réseau est proposée en annexe (cf. section 6.2).
[98] Le site au profit de Mike JONES a été créé et était hébergé par JMD avant la brouille entre les deux individus. Depuis, Mike JONES a débunké plusieurs des contenus de *Storm-1516*, et DOUGAN a attribué la paternité de certains noms de domaine du réseau à Mike JONES. Cf. https://www.thebureauinvestigates.com/stories/2024-07-06/russian-disinformation-networks-ramp-up-attacks-on-european-elections et https://gnidaproject.substack.com/p/disinformation-updates-cocaine-in. VIGINUM note par ailleurs que JMD a reçu plusieurs centaines de dollars de WESTALL *via* le service en ligne *Buymeacoffee* : https://archive.ph/YoYOg.
[99] 66.175.208[.]251, 69.164.216[.]69 et 95.165.66[.]27.

outils d'intelligence artificielle permettant de générer les articles reformulés. Depuis cette période, VIGINUM note une montée en compétences des opérateurs du réseau, ainsi qu'une amélioration de leurs procédures de sécurité opérationnelle, potentiellement avec l'appui technique du CEG et du GRU.

Depuis janvier 2024, les opérateurs de *CopyCop* exploitent de manière croissante les services d'anonymisation de *Cloudflare* et ont cessé de commettre des erreurs documentées dans des rapports publics[100]. Les faux sites exploitent généralement des services peu discriminants et sont hébergés sur des serveurs partagés, parfois dans le pays cible, à l'image du *cluster* de sites déposés chez l'hébergeur *SIM-Networks* pour cibler l'audience allemande. Les opérateurs réservent en outre un soin particulier à employer des *templates Wordpress* quasiment systématiquement différents, probablement dans le but de gêner la détection.

Si le réseau *CopyCop* fait aujourd'hui partie intégrante du mode opératoire *Storm-1516*, il est également exploité par d'autres acteurs et MOI du dispositif d'influence informationnelle russe. C'est notamment le cas de la « Fondation pour combattre l'injustice », structure du projet *Lakhta* (cf. section 4.2) qui publie une partie de ses « investigations » sur les sites du réseau, et de médias liés aux services de renseignement russes, tels qu'*Inforos*. En retour, les contenus mis en ligne sur le réseau ont déjà été amplifiés à plusieurs reprises par *RRN/Doppelgänger* et *Portal Kombat*[101].

4.2 Proximité avec la galaxie d'Evgueni PRIGOJINE

Storm-1516 possède des liens techniques forts avec des individus, des organisations et des modes opératoires informationnels liés au projet *Lakhta*. L'entreprise *Microsoft* estimait même en 2024 que le MOI serait une « excroissance » de l'*Internet Research Agency* (IRA) potentiellement opérée depuis Saint-Pétersbourg par des « vétérans » de l'IRA. Si VIGINUM ne peut confirmer l'ensemble de ces liens, il semble que des capacités historiquement liées à la galaxie aient été mises à contribution de *Storm-1516* après la mort d'Evgueni PRIGOJINE et la phase de restructuration de son dispositif informationnel, qui coïncide avec l'apparition du mode opératoire, en août 2023.

4.2.1 Liens avec la FCI et la BJA

L'analyse des opérations informationnelles de *Storm-1516* confirme que celles-ci sont quasi systématiquement amplifiées par des influenceurs liés à des organisations de la galaxie PRIGOJINE. Les plus actifs sont des membres ou contributeurs de la « Fondation pour combattre l'injustice » (FCI), une structure créée par PRIGOJINE en 2021 pour documenter les « violations des droits humains » dans les pays occidentaux, et de l'« Association des journalistes des BRICS » (BJA), qui dépend de la Fondation. Les deux organisations seraient gérées par Oksana VOVK, une ressortissante russe incarcérée deux ans aux États-Unis pour blanchiment, et agissant aujourd'hui sous le nom de Mira TERADA.

À titre d'exemple, les narratifs de *Storm-1516* sont presque tous relayés, quelques heures après leur primo-diffusion, par les comptes de réseaux sociaux et des sites liés à Chay BOWES, un journaliste pro-russe d'origine irlandaise ayant travaillé pour le groupe *RT* et vivant actuellement en Russie. Le mode opératoire s'appuie également sur Manish JHA, journaliste à la télévision indienne *TV9* et membre de la direction de la BJA, ainsi que sur un cercle restreint d'influenceurs américains, allemands, finlandais ou encore néerlandais qui entretiennent tous des liens avec la FCI et la BJA, et propagent les faux récits auprès d'audiences pro-Russes en différentes langues[102].

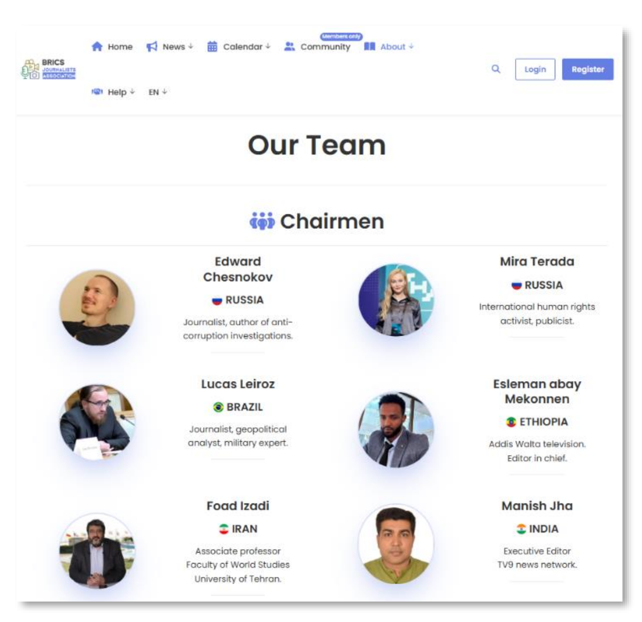
---

[100] https://archive.ph/AJyfi.

[101] https://harfanglab.io/insidethelab/doppelganger-operations-europe-us/ et https://www.voanews.com/a/7457286.html.

[102] Dont Alexandra READE, exilée en Russie depuis 2023, George ELIASON, Alina LIPP, administratrice de la chaîne *Telegram @neuesausrussland*, Jovica JOVIC, Sonja VAN DER ENDE, administratrice du site *devend.online*, et Janus PUTKONEN, éditeur en chef du site *mvlheti.net*.

Au regard des liens entre ces individus, ainsi que de la temporalité et du schéma d'amplification propre à *Storm-1516*, VIGINUM considère que ces reprises ne sont pas opportunistes, mais probablement sollicitées par un donneur d'ordre. Cette hypothèse est renforcée par l'implication directe de certaines personnalités dans le dispositif : Simeon BOÏKOV (*@aussiecossack*), australien d'origine russe réfugié dans le consulat russe de Sydney depuis 2022 et lié à la FCI, aurait servi de relais pour contacter et rémunérer au moins un influenceur américain en échange de la publication de contenus imputés à *Storm-1516* (cf. section 3.1.2).



Capture d'écran du site de la BJA

VIGINUM note par ailleurs que parmi les chaînes *Telegram* relayant quasi systématiquement les narratifs de *Storm-1516* auprès de l'audience russophone (cf. section 3.3), deux présentent des liens historiques avec le projet *Lakhta*. La chaîne *@golosmordora*, qui primo-diffuse le plus souvent les faux récits sur *Telegram*, était ainsi répertoriée parmi les « bloggeurs » de l'agence *RIA FAN*, principal média du groupe *Patriot* de PRIGOJINE[103]. La chaîne *@Radiostydoba* est quant à elle mentionnée dans les *Wagner Leaks* pour avoir été rémunérée en échange de publications[104]. Enfin, JMD et Valéry KOROVINE (cf. section 4.3.2) entretiennent des liens étroits avec Alekseï KIRISTAÏEV (aussi connu sous le nom d'Igor LOUKYANOV), qui a travaillé pour *RIA FAN* et le site *geopolitika.ru* (cf. section 4.3)[105].

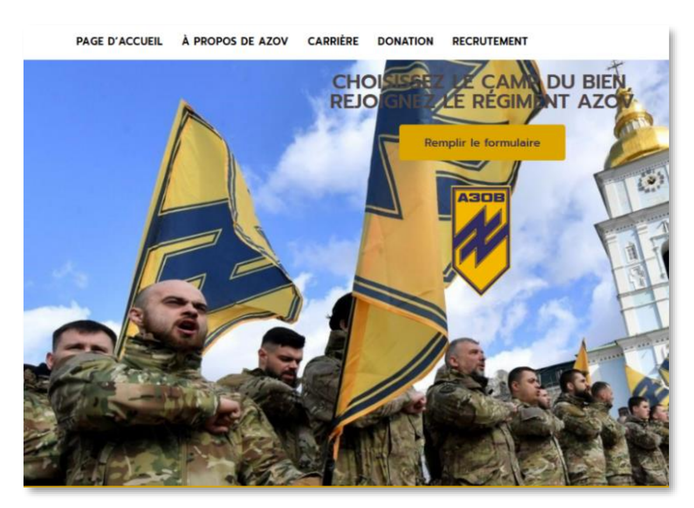
4.2.2 Liens avec le projet *Lakhta*

Storm-1516 a coordonné à plusieurs reprises ses opérations avec le projet *Lakhta*. Si le premier a reçu le soutien de comptes de réseaux sociaux liés au projet *Lakhta* durant les phases de primo-diffusion et d'amplification (cf. sections 3.1.2 et 3.3), les analyses de VIGINUM démontrent que *Storm-1516* a également soutenu, à deux reprises, des opérations initiées par *Lakhta*. Le 30 octobre 2023, *Storm-1516* a mis en ligne, blanchi puis amplifié le faux témoignage d'un ressortissant algérien déclarant s'être engagé dans le bataillon ukrainien Azov. Ce contenu semble en fait avoir servi à offrir de la visibilité au site *azov-france.fr*, enregistré le 20 octobre et que VIGINUM rattache avec un niveau de confiance élevé au projet *Lakhta*[106].

De la même façon, le mode opératoire *Storm-1516* a été employé fin décembre 2023 pour primo-diffuser et amplifier un faux *post* faisant la promotion d'un site ukrainien pro-transgenres déposé le 18 décembre, et imputé avec une confiance élevée par VIGINUM à *Lakhta* : *mytransitionua.org*[107]. Dans les deux cas, des comptes de *Lakhta* ont ensuite participé à l'amplification du contenu mis en ligne *via* *Storm-1516*. Ces deux opérations, qui n'ont pu être réalisées sans coordination, prouvent un degré significatif de coordination entre les deux modes opératoires informationnels.

[103] Cf. https://web.archive.org/web/20211117020613/riafan.ru/bloggers.
[104] Cf. https://dossier.center/prig-it/.
[105] Cf. https://gnidaproject.substack.com/p/john-dougans-cuban-connection-to et https://2017-2021.state.gov/russias-pillars-of-disinformation-and-propaganda-report.
[106] Cf. https://archive.ph/F54VT.
[107] Cf. https://archive.ph/jMIly.

Enfin, VIGINUM observe la réutilisation, par les opérateurs de *Storm-1516*, d'une série de TTP associées historiquement au projet *Lakhta*. Parmi ces derniers figurent le recours à des acteurs amateurs rémunérés pour crédibiliser des contenus[108], l'amplification *via* des commentaires dans des publications de médias occidentaux[109], ou encore le blanchiment de narratifs en rémunérant des sites africains. VIGINUM note ainsi qu'au moins 17 des médias exploités par *Storm-1516* avaient déjà été exploités par le projet *Lakhta*, dont *Elmostaqbal*, *NetAfrique*, ou *Tuko*[110]. Si ces emprunts peuvent paraître opportunistes, leur récurrence et leur reproduction à l'identique suggèrent qu'ils pourraient être issus de pratiques opérationnelles transmises par d'anciens opérateurs du projet *Lakhta*.



Capture d'écran d'une archive du site azov-france.fr

4.3 Proximité avec l'écosystème d'Aleksandr DOUGUINE

En outre, le mode opératoire présente des liens avec des individus et des organisations liées à Aleksandr DOUGUINE, philosophe ultra-nationaliste et anti-occidental russe. Dès mai 2024, le *New York Times* rapportait qu'un *think tank* moscovite, le Centre d'expertise géopolitique (CEG), était impliqué dans la conduite de *Storm-1516*. Le 31 décembre 2024, le CEG et son directeur, Valéry Mikhaïlovitch KOROVINE, ont été sanctionnés par le Trésor américain pour avoir « dirigé et subventionné la création et la publication de *deepfakes*, ainsi que la diffusion de fausses informations » visant les candidats à l'élection présidentielle américaine.

4.3.1 Le Centre d'expertise géopolitique (CEG)

Si VIGINUM n'est pas en mesure de confirmer l'implication directe du *think tank* dans le dispositif, des liens étroits ont pu être identifiés entre John Mark DOUGAN, le Centre d'expertise géopolitique, Valéry KOROVINE et Youry KHOROCHENKY, l'officier du GRU accusé publiquement de coordonner le mode opératoire (cf. section 4.4). Le CEG est un centre de réflexion fondé par DOUGUINE au début des années 2000[111], qui affirme proposer des services de conseil en « risque pays » à des industries du secteur privé, et disposer de représentants « dans tous les pays de la Communauté des États indépendants, ainsi qu'en Europe, en Asie, et au Moyen-Orient ».

Le CEG est lié depuis ses débuts à « *Evrazia* », un parti politique néo-eurasiste créé par DOUGUINE en 2002. Si le CEG possédait son propre site depuis 2010, qui ne contient que les statuts du « fonds non-commercial international »[112], sa page principale est hébergée depuis au moins 2003 sur un sous-domaine du portail d'information officiel du parti politique, *cge.evrazia.org*, qui arbore par ailleurs son logo[113]. *Evrazia* constitue aujourd'hui une plateforme pour les différentes initiatives et mouvements de DOUGUINE, qui coordonne également, entre autres, l'Union de la jeunesse eurasienne et le Mouvement eurasien international.

---

[108] https://web.archive.org/web/20211106004546/https://twitter.com/Jay_Belichick/status/1456784722659586050.
[109] Cf. https://www.cardiff.ac.uk/__data/assets/pdf_file/0007/2551849/final-report.pdf.
[110] Cf. https://www.aljazeera.com/features/2025/3/20/the-ghost-reporters-writing-pro-russian-propaganda-in-west-africa.
[111] https://www.state.gov/wp-content/uploads/2022/01/LS-2020-0111499-PILLARS-OF-RUSSIA-DISINFORMATION-FRE.pdf.
[112] https://web.archive.org/web/20190326084451/http://cge.su/.
[113] https://web.archive.org/web/20030806182525/http://cge.evrazia.org/about.shtml.

Les enregistrements DNS historiques prouvent que le nom de domaine d'*Evrazia* résolvait des adresses IPv4[114] liées à une galaxie de sites visiblement administrés par DOUGUINE, KOROVINE et leurs équipes. VIGINUM a notamment pu identifier, à partir d'archives en ligne, des sites personnels, liés à différents mouvements et emprises locales d'*Evrazia*, à des partis politiques, à des églises orthodoxes, à des groupes anarchistes, à un centre de l'Université d'État de Moscou, à des portails « philosophiques », ainsi que des sites d'information régionaux axés en particulier sur l'Ukraine et le projet « Novorossiya »[115]. Pour une raison inconnue, ce *cluster* comprenait également plusieurs sites d'entreprises privées russes, ainsi que des noms de domaine n'ayant manifestement jamais été exploités[116].



Photo de DOUGAN (à gauche) et KOROVINE (à droite) à un événement de la Fondation Fidel Castro

4.3.2 Valéry KOROVINE

Dès sa création, le CEG aurait été dirigé par Valéry KOROVINE, un journaliste et politologue russe travaillant avec DOUGUINE depuis au moins 1995. À partir de 2001, il aurait dirigé les sections de l'information d'*Evrazia* et du Mouvement eurasien international, avant de prendre la tête de l'Union de la jeunesse eurasienne en 2005. KOROVINE est aujourd'hui actif dans de nombreux cercles de réflexion proches du gouvernement russe, dont le Club d'Izborsk (aux côtés de DOUGUINE), le mouvement « Rêve russe », ou encore la Fondation Fidel Castro, dont le site était hébergé sur l'infrastructure de *CopyCop*, et créée par Léonid SAVINE, éditeur en chef de *geopolitika.ru*.

Depuis au moins 2021, KOROVINE a participé à de nombreux événements auxquels John Mark DOUGAN était présent, dont des conférences sur « les guerres des réseaux dans l'espace post-soviétique », l'influence turque dans le Caucase, ou encore le « programme de développement d'armes bactériologiques américano-ukrainien ». En parallèle, KOROVINE aurait, depuis 2022, financé et travaillé avec des journalistes étrangers pour qu'ils présentent une image positive de l'invasion de l'Ukraine, en organisant notamment des voyages dans les territoires ukrainiens occupés[117].

D'après les éléments révélés par le *Washington Post* en octobre 2024, KOROVINE aurait envoyé une lettre en 2019 au ministère de la Défense russe pour proposer que le CEG organise « une guerre Internet contre les États-Unis sur son propre territoire ». Depuis au moins 2022, KOROVINE participerait à des réunions fréquentes avec DOUGAN et un officier du GRU, Youry KHOROCHENKY, présenté comme le directeur-adjoint du CEG (cf. section 4.4), dans le but de coordonner les opérations informationnelles de *Storm-1516*[118]. Le Trésor américain suggère que le CEG serait responsable de la création et de la dissémination des contenus du MOI, et aurait mis en place le serveur permettant de les générer artificiellement[119].

---

[114] Dont 195.210.167[.]67 entre 2013 et 2015, 86.62.112[.]120 entre 2015 et 2021, et 93.95.101[.]235 entre 2015 et 2024.

[115] Parmi ces noms de domaine figurent les sites de DOUGUINE et de MAKEÏEVA, bras droit de KOROVINE (*dugin.ru* et *makeeva.net*), du mouvement (*4theory.ru*, *rossia3.ru*, *skavkaz.info*, *chaosmage.ru*, *med.org.ru*, *referendumunion.ru*, etc.), du Front national-bolchévique (*nbf.org.ru*), ou encore *arctogaia.net.ru*, *anarh.ru*, *rusila.su*, *vehi.tv*, *konservatizm.org* et *maloros.ru*.

[116] Dont *geopolitika.tv* et *nazarbaev.ru*. Ce dernier pourrait être lié à l'ancien président du Kazakhstan Noursoultan NAZARBAÏEV.

[117] https://www.valisluureamet.ee/doc/raport/2024-en.pdf.

[118] https://www.washingtonpost.com/world/2024/10/23/dougan-russian-disinformation-harris/.

[119] https://home.treasury.gov/news/press-releases/jy2766.

Les liens entre ces différents acteurs et structures sont encore renforcés par le fait qu'ils exploitent les mêmes locaux, situés au 11 allée Bryoussov, bâtiment 1, bureau 314[120], dans le centre de Moscou. Cette adresse est en effet renseignée dans les contacts du CGE, du Mouvement eurasien international, de la Fondation Fidel Castro, de *geopolitika.ru* et du Club économique eurasien, un projet historiquement lié à DOUGUINE et aujourd'hui conduit par Mikhaïl ANISSIMOV, entrepreneur également actif dans la Fondation Fidel Castro et le mouvement « Rêve russe »[121]. Enfin, le lieu a été exploité pour réaliser des vidéos de John Mark DOUGAN, et notamment des interviews de Tim KIRBY, dont le site était également hébergé sur le réseau *CopyCop*[122].

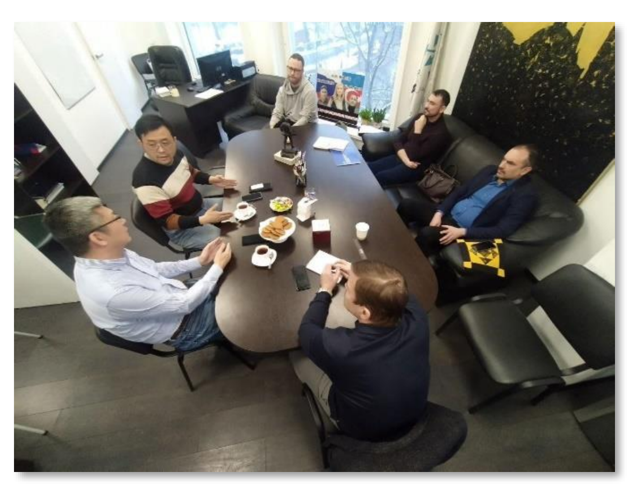


Photo des locaux situés au 11 allée Bryoussov durant une réunion entre ANISSIMOV, le ministère de la défense russe et des industriels chinois

Au-delà de cet écosystème agissant depuis le territoire russe, VIGINUM a observé que des individus étrangers proches de la galaxie DOUGUINE avaient participé à des opérations informationnelles de *Storm-1516*. C'est notamment le cas de Raphael MACHADO et Lucas LEIROZ, respectivement président et membre de l'organisation nationaliste brésilienne *Nova Resistência*, proche de DOUGUINE[123], qui ont amplifié au moins huit opérations informationnelles du MOI entre août 2023 et janvier 2025. Lucas LEIROZ fait en outre partie du bureau de la BJA (cf. section 4.2), et a collaboré avec *Inforos*[124], une agence d'information attribuée publiquement à l'unité 54777 du GRU[125].

4.4 Un MOI potentiellement coordonné par un service de renseignement russe

Selon les documents obtenus par le *Washington Post* auprès d'un service de renseignement européen, le ressortissant russe Youry KHOROCHENKY[126] est accusé d'avoir financé et coordonné les opérations du mode opératoire depuis son apparition. Toujours selon la même source, KHOROCHENKY, qui évoluerait parfois sous le nom de Youry KHOROCHYOVSKY[127], serait en fait un officier de l'unité 29155 du renseignement militaire russe (GRU), une unité de type « action » historiquement et publiquement liée à des opérations de sabotage, à des tentatives d'assassinat, à la distribution de primes pour la mort de soldats de l'OTAN en Afghanistan, à des tentatives de coup d'État en Europe, à des opérations d'espionnage et de sabotage informatique, et qui serait, selon des éléments récents, responsable du syndrome de La Havane[128].

KHOROCHENKY aurait effectué des transactions financières vers le compte bancaire de JMD dès avril 2022, et participerait à des réunions régulières avec John Mark DOUGAN et Valéry KOROVINE. Fin décembre 2024, le Département du Trésor américain a confirmé que le GRU avait coordonné et

---

[120] En russe, Брюсов переулок, д. 11/1, офис 314.
[121] https://web.archive.org/web/20240323094129/http://anisimov.co/.
[122] https://gnidaproject.substack.com/p/john-dougans-cuban-connection-to.
[123] https://www.state.gov/wp-content/uploads/2023/10/Nova-Resistência-in-Brazil_Oct_25_23_508.pdf.
[124] https://openfacto.fr/2022/10/24/inforos-les-reseaux-historiques-dinfluence.
[125] https://www.europarl.europa.eu/doceo/document/E-9-2020-003669_EN.html.
[126] En russe, Юрий ХОРОШЕНЬКИЙ.
[127] En russe, Юрий ХОРОШЕВСКИЙ.
[128] https://static.rusi.org/SR-Russian-Unconventional-Weapons-final-web.pdf.

soutenu les opérations du Centre d'expertise géopolitique, en suggérant l'implication de l'unité 29155, mais sans mentionner le nom de KHOROCHENKY.

VIGINUM n'est pas en mesure de confirmer l'implication directe de KHOROCHENKY ou de l'unité 29155 dans la conduite de *Storm-1516*. Toutefois, des investigations complémentaires du service ont permis de mettre en lumière des liens étroits entre cet individu et les écosystèmes susmentionnés.

VIGINUM a ainsi identifié qu'un certain « Youry Timofeïevitch KHOROCHYOVSKY » apparaissait dans le programme d'une conférence organisée en octobre 2022 par l'Université d'État de linguistique de Moscou à laquelle participaient également DOUGAN, KOROVINE et SAVINE. KHOROCHYOVSKY était alors présenté comme le directeur-adjoint du Centre d'expertise géopolitique et directeur-adjoint du Club économique eurasien[129]. Des recherches à partir du prénom, du patronyme et du nom connu de l'officier (KHOROCHENKY) ont permis d'obtenir des informations supplémentaires sur cet individu et ses liens potentiels avec le GRU.

Des fuites de données accessibles publiquement suggèrent l'existence d'un Youry Timofeïevitch KHOROCHENKY, né le 30 novembre 1978[130]. VIGINUM note que l'adresse renseignée par l'individu, « 76B, route Khorochyovskoïe »[131], correspond à celle du quartier-général du GRU. Sans qu'il soit possible d'attester qu'il s'agisse bien d'une erreur de sécurité opérationnelle commise par l'officier, cette adresse a déjà permis à des journalistes d'investigation d'identifier des membres du GRU – dont de l'unité 29155 – à partir de données fuitées ou achetées[132].

[129] https://archive.ph/jSPkZ.
[130] https://ghostarchive.org/archive/xuzoM.
[131] En russe, Хорошевское шоссе, д. 76Б.
[132] Cf. investigations de *Bellingcat* sur l'unité 29155 : https://www.bellingcat.com/news/uk-and-europe/2018/10/08/second-skripal-poisoning-suspect-identified-as-dr-alexander-mishkin/.

5. CONCLUSION

Actif depuis plus d'un an et demi, *Storm-1516* est un mode opératoire informationnel qui peut être considéré comme particulièrement complexe, adaptable, et efficace pour diffuser des narratifs anti-Ukrainiens et anti-Occidentaux auprès d'audiences occidentales.

L'analyse par VIGINUM de ses opérations informationnelles démontre que le dispositif d'influence informationnelle russe a investi des efforts conséquents pour coordonner les actions d'un important réseau d'acteurs, d'organisations et de MOI agissant depuis le territoire russe et dans les pays ciblés, et ce depuis le début de l'invasion à grande échelle de l'Ukraine par la Russie en 2022.

Storm-1516 constitue aujourd'hui un mode opératoire informationnel cohérent et mature, qui offre à ses commanditaires la capacité de mener à la fois des actions de court terme en réaction à l'actualité, mais également de s'inscrire dans des stratégies de long terme, visant à décrédibiliser des personnalités ou des organisations européennes et nord-américaines – notamment en amont de grands événements et de processus électoraux.

Si l'impact réel du mode opératoire sur le débat public numérique demeure difficile à estimer, VIGINUM observe que de nombreux narratifs propagés *via* le MOI ont atteint une visibilité très importante en ligne, et qu'ils sont parfois repris, de manière inconsciente ou opportuniste, par des personnalités et des représentants politiques de premier plan.

Les opérateurs de *Storm-1516* poursuivent aujourd'hui leurs activités avec un rythme opérationnel soutenu, et devraient très probablement continuer à adapter leurs TTPs, notamment pour crédibiliser davantage leurs contenus, tenter de contourner les mécanismes de modération des plateformes, gêner le suivi et l'imputation technique de leurs activités, ou encore renouveler leurs infrastructures d'attaque.

Au regard de ces éléments, **VIGINUM considère que les activités de *Storm-1516* réunissent les critères d'une ingérence numérique étrangère, et représentent une menace importante pour le débat public numérique français et européen**.

6. ANNEXES

6.1 Opérations imputées à *Storm-1516*

N°	Titre	Date	Primo-diffusion
1	La belle-mère de Volodymyr ZELENSKY possède une villa en Égypte	20 août 2023	https://www.youtube.com/watch?v=cCEUdUBHPkE
2	Le prince Andrew a agressé sexuellement et enlevé des enfants ukrainiens	27 août 2023	https://ghostarchive.org/varchive/1-nU-7vZmVA
3	Des soldats de l'OTAN ont agressé sexuellement une Allemande d'origine turque	17 septembre 2023	https://archive.ph/Xt5C2
4	Volodymyr ZELENSKY participe à des orgies	23 septembre 2023	https://archive.ph/vfBQg
5	Le gouvernement ukrainien recrute des combattants de l'État islamique	27 septembre 2023	https://archive.ph/5KpGG
6	Olena ZELENSKA a dépensé 1,1 million de dollars dans la boutique Cartier de New York	30 septembre 2023	https://archive.is/xCaa6
7	Le gouvernement ukrainien planifie une attaque contre l'ambassade allemande à Kyiv	18 octobre 2023	https://archive.ph/y2Y3t
8	Le gouvernement ukrainien a envoyé des armes au Hamas	28 octobre 2023	https://facebook.com/roxanne.pounds.9/videos/1294280007941235
9	Le bataillon Azov recrute des combattants en France	30 octobre 2023	https://archive.ph/WmHkv
10	Le bataillon Azov s'entraîne avec le Hamas	2 novembre 2023	https://archive.ph/gm4hg
11	La Fondation ZELENSKA est impliquée dans le trafic d'enfants ukrainiens	3 novembre 2023	https://archive.ph/7CS3K
12	Volodymyr ZELENSKY est propriétaire de deux yachts d'une valeur de 75 millions de dollars	23 novembre 2023	https://archive.ph/O2Ppq
13	Le gouvernement ukrainien est impliqué dans le trafic d'organes de soldats	27 novembre 2023	https://archive.ph/WjhJs
14	Volodymyr ZELENSKY et George SOROS ont passé un accord pour l'enfouissement de déchets toxiques en Ukraine	27 novembre 2023	https://archive.ph/jx5hG

15	Volodymyr ZELENSKY a acquis une propriété en Floride avec l'aide de l'*U.S. Secret Service*	29 novembre 2023	https://archive.ph/7jA5j
16	Volodymyr ZELENSKY critique des dirigeants occidentaux dans un appel téléphonique fuité	6 décembre 2023	https://web.archive.org/web/20231207215607/youtube.com/watch?v=Rg7XoA_I-OI
17	Volodymyr ZELENSKY a fait assassiner un journaliste égyptien travaillant sur la corruption	21 décembre 2023	https://ghostarchive.org/varchive/wBmPBznhis8
18	Volodymyr ZELENSKY soutient une initiative pro-transgenres	23 décembre 2023	https://archive.ph/MhhMW
19	Volodymyr ZELENSKY a acquis l'ancienne ville de GOEBBELS	24 décembre 2023	https://archive.ph/adzvm
20	Volodymyr ZELENSKY a acheté des peintures surévaluées d'Hunter BIDEN	28 décembre 2023	https://archive.ph/c9ODv
21	Léonid VOLKOV a dépensé 40 000 euros dans un restaurant	28 décembre 2023	https://archive.ph/5escN
22	Le gouvernement ukrainien développe secrètement des armes nucléaires avec de l'uranium nigérien fourni par Orano	22 janvier 2024	https://ghostarchive.org/varchive/kdHx4eXHoj8
23	Volodymyr ZELENSKY a acquis un appartement à Dubaï	23 janvier 2024	https://archive.ph/PdPI5
24	Des tests de vaccins COVID Pfizer ont provoqué la mort de 40 enfants ukrainiens	3 février 2024	https://archive.ph/seZC8
25	Youlya NAVALNAÏA entretient des relations extra-conjugales	3 février 2024	https://archive.ph/nL5MR
26	Le gouvernement ukrainien a tenté d'assassiner Tucker CARLSON	25 février 2024	https://archive.ph/3RvqA
27	Le gouvernement américain finance l'opposition russe	27 février 2024	https://archive.ph/9klbX
28	Des producteurs d'Hollywood préparent un film en l'honneur de Volodymyr ZELENSKY	27 février 2024	https://archive.ph/9dnc1
29	Léonid VOLKOV vend des réfugiées Ukrainiennes à des réseaux de prostitution	2 mars 2024	https://ghostarchive.org/archive/Zyq9P
30	Le mode opératoire informationnel *RRN/Doppelgänger* est conduit par le département d'État américain	7 mars 2024	https://archive.ph/N2o6M
31	Léonid VOLKOV a été agressé en Lituanie par son ancien amant	15 mars 2024	X

32	Volodymyr ZELENSKY a importé illégalement de la cocaïne d'Argentine	21 mars 2024	https://archive.ph/fk7MZ
33	Volodymyr ZELENSKY a acquis une ancienne propriété de Charles III	31 mars 2024	https://archive.is/BuMj1
34	La CIA conduit une ferme à trolls pro-BIDEN depuis Kyiv	19 avril 2024	https://archive.ph/P3TZ8
35	Le FBI a mis sur écoute la résidence de Donald TRUMP	25 avril 2024	https://archive.ph/RIHW7
36	Des soldats ukrainiens ont brûlé un mannequin à l'effigie de Donald TRUMP	2 mai 2024	https://archive.ph/3cHQu
37	La ville de Paris a renommé un pont en l'honneur de l'Armée rouge	5 mai 2024	https://archive.md/AL74r
38	Ursula VON DEY LEYEN est impliquée dans un schéma de contournement des sanctions contre la Russie	26 mai 2024	https://ghostarchive.org/varchive/LqPZUoYFP1g
39	Un manifestant pro-Palestinien a été tué par la police à Paris	27 mai 2024	https://archive.ph/gLorg
40	Volodymyr ZELENSKY a acquis un casino à Chypre	1er juin 2024	https://archive.ph/Zfyyz
41	La coalition « Ensemble » propose 100 euros aux électeurs français en amont des élections législatives anticipées	26 juin 2024	https://archive.ph/V1z0x
42	Olena ZELENSKA a acquis une voiture de luxe	1er juillet 2024	X
43	Des Ukrainiens ont vandalisé une mosquée en Allemagne en soutien à Israël	4 juillet 2024	https://archive.ph/Yna6M
44	Le Hamas menace de conduire des attaques durant les JOP2024	21 juillet 2024	https://ghostarchive.org/archive/peUKO
45	Annalena BAERBOCK a profité de services sexuels en Afrique	29 juillet 2024	https://archive.ph/kRgYN
46	Barack OBAMA est impliqué dans la tentative d'assassinat contre Donald TRUMP	1er août 2024	https://web.archive.org/web/20240806023710/https://deepstateleaks.org/top-democrats-are-behind-the-assassination-attempt-on-trump-obama-knows-about-the-details/
47	Volodymyr ZELENSKY a acquis la villa du chanteur Sting en Italie	5 août 2024	https://archive.ph/GKuXc
48	Des soutiens de Donald TRUMP ont été agressés par des soutiens de Kamala HARRIS	30 août 2024	X

49	Kamala HARRIS est responsable d'un accident de la route grave en 2011	2 septembre 2024	https://archive.ph/OtkK3
50	George SOROS et Bill GATES font partie de l'équipe de campagne de Kamala HARRIS	24 septembre 2024	https://archive.ph/vSglt
51	Kamala HARRIS participe à des safaris d'animaux menacés en Afrique	24 septembre 2024	https://archive.ph/ZAVjC
52	Kamala HARRIS est cocaïnomane	2 octobre 2024	https://ghostarchive.org/archive/iQHZL
53	Donald TRUMP a fait des dons à un institut de lutte contre le cancer	4 octobre 2024	https://ghostarchive.org/archive/D5wOg
54	Volodymyr ZELENSKY a acquis l'ancienne voiture d'Adolf HITLER	7 octobre 2024	https://archive.ph/11zsS
55	Timothy WALTZ a agressé sexuellement un ancien élève	16 octobre 2024	https://archive.is/rnvuH
56	Des bulletins en faveur de Donald TRUMP ont été détruits dans un bureau de vote en Pennsylvanie	24 octobre 2024	https://archive.md/2GcTf
57	Kamala HARRIS a prévenu un rappeur et producteur avant la perquisition de son domicile	30 octobre 2024	https://archive.is/Mfja0
58	Des immigrés haïtiens ont voté illégalement pour Kamala HARRIS	31 octobre 2024	https://archive.is/94iT3
59	Marcus FABER est un agent russe	5 novembre 2024	https[:]//anderemeinung[.]de/2024/11/arbeitet-verteidigungsausschuss-chef-faber-fuer-russland-vorwurf-video-aufgetaucht/
60	Un soutien de Donald TRUMP a été agressé dans un bureau de vote	5 novembre 2024	https://archive.ph/Tc6Wg
61	L'armée allemande prévoit de recruter 500 000 soldats pour garantir la paix en Europe de l'Est	19 novembre 2024	https://archive.ph/6ktsw
62	Volodymyr ZELENSKY a acquis un hôtel à Courchevel	25 novembre 2024	https://archive.ph/tCzgE
63	Robert HABECK a agressé sexuellement une écolière en 2017	6 décembre 2024	https://archive.is/SsT4k
64	Robert HABECK a signé un accord pour l'arrivée en Allemagne de 1,9 million de travailleurs kényans	17 décembre 2024	https://archive.ph/6q8Yr
65	Un immigré tchadien accusé de viol sur mineure a été relâché par la police française	23 décembre 2024	https://ghostarchive.org/archive/IT3YV

TLP:CLEAR

66	Ryan ROUTH coopère avec le renseignement ukrainien	3 janvier 2025	https://ghostarchive.org/archive/gyQW8
67	Volodymyr ZELENSKY a acquis une ville à Saint-Barthélemy	7 janvier 2025	https://ghostarchive.org/archive/mSw8a
68	Les missiles russes *Orechnik* posent un enjeu de sécurité à l'OTAN	9 janvier 2025	https://archive.ph/nNQfY
69	Une Allemande portée disparue a été assassinée par un islamiste	22 janvier 2025	https://x.com/MuhammadAliZu/status/1881953455688081727
70	Le groupe Hayat Tahrir-al-Cham menace d'attaquer Notre-Dame de Paris	26 janvier 2025	https://ghostarchive.org/archive/cNzzs
71	Robert HABECK et Claudia ROTH impliqués dans une affaire de corruption concernant des œuvres d'art	30 janvier 2025	https://archive.ph/hOL61
72	Friedrich MERZ aurait des troubles mentaux	3 février 2025	https://archive.is/sIeDD
73	Volodymyr ZELENSKY a acquis le « nid d'aigle » d'Adolf HITLER	5 février 2025	https://archive.is/63RI7
74	Le parti allemand *AfD* est absent de certains bulletins de vote	18 février 2025	https://archive.ph/Qe5HV
75	Des bulletins de vote en faveur de *l'AfD* ont été détruits	20 février 2025	https://archive.ph/DoZd2
76	Brigitte MACRON a agressé sexuellement un ancien étudiant	28 février 2025	https://archive.ph/t5Suz
77	Volodymyr ZELENSKY a acquis la banque française *Milleis*	5 mars 2025	https://archive.ph/Z815H

6.2 Noms de domaine liés à *CopyCop*

1776.chat
aktuellde.de
aktuellenews-berlin.de
aktuelles-aus-nurnberg.de
aktuell-nachricht.de
alles-klar-hamburg.de
alles-wichtig-news.de
allethemen24.de
american-freedom.org
an-berlin.de
anderemeinung.de
andererseits-seite.de
atlantabeacon.org
atlanta-observer.com
ausdemueberall.de
austincrier.com
badvolf.com
badvolf.ru
bbc-uk.news
b-blatt.de
berlin-apropos.de
berlinertagespost.de
berliner-wochenzeitung.de
bostontimes.org
botbook.us
britishchronicle.com
brlnr-stimme.de
capitolpulse.com
carsondispatch.com
casinohotelvunipalace.com
centernewscentral.com
centerpointbeacon.com
centralrecord.org
chicagochron.com
chicagocrier.com
cito-novit.de
civiccentury.org
civiccommentary.org
civiccorner.org
civiccreed.com
civiccurrent.com
civiccurve.com
clearstory.news
conservativecamp.org
conservativecatch.org
conservativechannel.org
conservativecircuit.com
conservativecompass.org
conservativecontext.com
conservativecorridor.com
conservativecourier.org
dailyregisternews.com
das-denkt-hamburg.de
dasneueste-online.de
daybreakdigest.org
dc-free-press.org
dcweekly.org
deepstateleaks.org
deinequellen.de
democracydepth.com
democracydive.com
democracydrive.org
de-nachrichtenseite.de
desmoinesdefender.com
deutschenachrichtenstelle.de
deutsch-w.de
dhstalk.com
diamondadvertiser.com
diewahreseite.de
disnitsa.com
doch-infomedia.de
dznachrichten.de
echozeit.com
edatew.com
einfachandersinfo.de
einmaleinsneu.de
elbevets.com
ensemble-24.fr
epochpost.org
expert-infomedien.de
f-aktuell.de
falconeye.tech
fcastro.ru
flagstaffpost.com
flyoverbeacon.com
flythesky.ru
foreignagentintel.com
franceencolere.fr
freedomfacade.com
freedomfixture.com
freedomforge.info
freedomfoundry.info
freeeaglepress.org
fr-press.de
gaugerformayor.com
gbgeopolitics.com
gegengewicht-media.de
gegenleitmedien.de
georgiagazette.us
gopguardian.com
governancegaze.com
greenmen-movement.com
guckmalgenauhin.de
hamb-post.de
hamburger-anzeiger.de

hamburger-sichtweisen.de
hamburg-ex.de
harrisburg-chronicle.com
heartlandharbor.org
heartlandhaven.org
heartlandheadlines.net
heartlandherald.us
heartland-inquirer.org
herrpostillon.de
heute-inberlin.de
h-np.de
honestcitizens.org
hotelpalacedesneiges.com
houstonpost.org
in-absicht.de
infomediafuerdich.de
info-mediaplattform.de
infomediaregierungskritisch.de
informant-info.de
infosindependants.fr
info-stichpunkt.de
ins-gesicht.de
internetpoebler-info.de
in-und-ausland.de
justiceserved.org
kbsf-tv.com
kernpunkt-infomedia.de
kernrecht.de
klartext-news.de
konusnews.de
kurzchronik.de
la-cher.de
lakestarreview.com
langmir.ru
lansingtribune.org
laut-medien.de
leaderledger.net
leaveukrainewar.com
lesechodelafrance.fr
libertylagoon.org
libertylantern.org
libertylaunch.org
libertylectern.org
libertypressnews.com
libertyvoice.info
londonchronicle.news
londoncrier.co.uk
londoncrier.com
lonestarcrier.com
ltcolstu.com
madison-gazette.org
media-transparent.de
mehrstimmen.de
miamichron.com
michigantribune.org
munchener-nachrichten.de
mytransitionua.org
nachrichtendestages.de
nachrichtenunabhaengig.de
n-a-h.de
nationalcrier.com
nationalmatters.org
nationalnarrative.org
nationnotebook.com
nebraskatruth.com
nevadaannouncer.com
nevadaannouncer.org
newscenterpress.org
news-checker.de
newsdesk.press
newsfuereuch.de
newsletters-berlin.de
newsmacher.de
newswichtig.de
newwayforward.us
newwayforward.vote
niggar.tech
nnberlin.de
northcarolinacourier.us
novanachrichten.de
nrtv.online
nudis-verbis.de
nynewsdaily.org
oakjournalnews.com
oasisobserverpost.org
oasis-weekly-post.com
oku-nachrichten.de
onlinedaheim-24.de
onlineunterwegs.de
oraclenews.org
parler2.com
partyperspective.com
patriotbeacon.us
patrioticpage.com
patrioticparade.com
patrioticpioneer.com
patrioticpulse.info
patriotvoicenews.com
pbsotalk.org
pennsylvaniamessenger.com
phoenixpatriot.org
polemisch-infomedia.de
policypaddock.com
policypassage.com
policypatch.com
policypath.org
policypeak.org
policyplatform.info
policyporch.org
politicalpioneer.com
politicalplot.org

politicalporch.com
politicostream.com
presseneu.de
prinzipienfest.de
proudamerican.cc
publicnewspaper.org
pulsepress.org
purplestatepost.com
raleigh-herald.com
red-blue-tribune.com
redo1776.com
redstategazette.com
redstatereport.net
republicrally.com
republicrange.com
republicregard.com
republicreview.net
republicripple.com
republicroot.com
republicroots.org
republicrundown.com
resonieren.de
rightrealm.net
rightresonance.org
rightreview.org
rightrevival.org
rightrundown.com
rightwingrev.com
ruf-der-freiheit.de
rundumdieuhr-24.de
sag-das.de
sanfranchron.com
sarahwestall.com
sarahwestall.org
scheinwerfen.de
scopestory.com
seattle-tribune.com
seite-eins-nachrichten.de
senatesight.com
signaldaily.org
silverstatesignal.org
skryty.ru
soiij.org
speech.chat
statestage.org
stimmedeutsch.de
suitreview.org
tageblatt-berlin.de
tagesnews-24.de
tagundnacht24.de
thearizonaobserver.com
thegeorgiangazette.com
thegreenmen.org
thesis-info.de
todayschronicle.org
top-news-munchen.de
tribunetimes.org
truthapedia.com
truthapedia.org
truthcentral.org
turnsy.com
ukpoliticking.com
ukrainepeace.org
ungeziert-info.de
unitytrend.com
unmittelbar-medien.de
vanguardviews.com
veritecachee.fr
vidvist.com
visionar-info.de
vollverstand.de
votervista.net
w-a-munchen.de
warstudiescentre.co.uk
washingtonwatch.us
wdr-hall.de
wehrpflicht2025.de
weitwinkelmedien.de
woodlandweeklyguardian.com
worldnewsdesk.press
xn--wochenberblick-berlin-eic.de
xposedem.com
zeitenwende-news.de
zeitgeschenen.de

6.3 Comptes et médias tiers impliqués

6.3.1 Médias exploités pour le blanchiment

actucameroun.com
almashhad-alyemeni.com
almasryalyoum.com
dailypost.ng
elaosboa.com
elbashayer.com
elmostaqbal.com
iharare.com
independent.ng
maliactu.net
malijet.com
muhtwaplus.com

mynewsgh.com

naijaloaded.com.ng

netafrique.net

newsghana.com

punchng.com

senenews.com

thenationonlineng.net

thesouthafrican.com

togoweb.net

tuko.co.ke

6.3.2 Canaux exploités durant la primo-diffusion et l'amplification

Dans cette section figurent uniquement les canaux (sites et comptes de réseaux sociaux) que VIGINUM a identifié au cours de plusieurs opérations informationnelles de *Storm-1516*, et considérés comme ayant été probablement rémunérés ou activés par les opérateurs du MOI :

devend.online

farodiroma.it

islanderreports.substack.com

mainland.press

mvlehti.net

news9live.com

odatv.com

odatv4.com

okv-ev.de

on4haber.com

russland-aktiv.de

t.me/AussieCossack

t.me/golosmordora

t.me/michel_mickael_wittwer

t.me/neuesausrussland

t.me/radiostydoba

t.me/sanya_florida

t.me/warhistoryalconafter

theinteldrop.org

theislander.eu

tv9hindi.com

uvmedia.org

vtforeignpolicy.com

x.com/AdrienBocquet59

x.com/AlertChannel

x.com/Alphafox78

x.com/ANN_News92

x.com/aussiecossack

x.com/camaradamachado

x.com/ChayBowes

x.com/daniel_gugger

x.com/DD_Geopolitics

x.com/gheliason

x.com/IslanderReports

x.com/its_The_Dr

x.com/janus_putkonen

x.com/JimFergusonUK

x.com/JovicaJovic15

x.com/leiroz_lucas

x.com/MichelMichaelW1

x.com/MiraMiru4

x.com/MyLordBebo

x.com/ReadeAlexandra

x.com/simonateba

x.com/SonjaEnde

x.com/TheWakeninq

x.com/vtforeignpolicy

x.com/Zlatti_71

6.4. Tactiques, techniques et procédures employées

[TA01] Plan Strategy

- [T0073] Determine Target Audiences

- [T0074] Determine Strategic Ends

[TA02] Plan Objectives

- [T0002] Facilitate State Propaganda

- [T0066] Degrade Adversary

- [T0075] Dismiss

- [T0075.001] Discredit Credible Sources

- [T0076] Distort

- [T0077] Distract

- [T0078] Dismay

- [T0079] Divide

[TA14] Develop Narratives

- [T0003] Leverage Existing Narratives

- [T0022] Leverage Conspiracy Theory Narratives

- [T0022.001] Amplify Existing Conspiracy Theory Narratives

- [T0022.002] Develop Original Conspiracy Theory Narratives

- [T0082] Develop New Narratives

- [T0083] Integrate Target Audience Vulnerabilities into Narrative

[TA06] Develop Content

- [T0023] Distort Facts
- [T0023.001] Reframe Context
- [T0084] Reuse Existing Content
- [T0084.002] Plagiarise Content
- [T0085] Develop Text-Based Content
- [T0085.001] Develop AI-Generated Text
- [T0085.002] Develop False or Altered Documents
- [T0085.003] Develop Inauthentic News Articles
- [T0086] Develop Image-Based Content
- [T0086.003] Deceptively Edit Images (Cheap Fakes)
- [T0087] Develop Video-Based Content
- [T0087.001] Develop AI-Generated Videos (Deepfakes)
- [T0088] Develop Audio-Based Content
- [T0088.001] Develop AI-Generated Audio (Deepfakes)

[TA15] Establish Social Assets

- [T0013] Create Inauthentic Websites
- [T0090] Create Inauthentic Accounts
- [T0090.001] Create Anonymous Accounts
- [T0093] Acquire/Recruit Network
- [T0093.001] Fund Proxies

[TA16] Establish Legitimacy

- [T0009] Create Fake Experts
- [T0097] Create Personas
- [T0097.001] Produce Evidence for Persona
- [T0098] Establish Inauthentic News Sites
- [T0098.001] Create Inauthentic News Sites
- [T0098.002] Leverage Existing Inauthentic News Sites
- [T0099] Impersonate Existing Entity
- [T0099.003] Impersonate Existing Organisation
- [T0099.004] Impersonate Existing Media Outlet
- [T0099.005] Impersonate Existing Official
- [T0100] Co-Opt Trusted Sources
- [T0100.001] Co-Opt Trusted Individuals
- [T0100.003] Co-Opt Influencers

[TA07] Select Channels and Affordances

- [T0104] Social Networks
- [T0104.001] Mainstream Social Networks
- [T0104.004] Interest-Based Networks
- [T0105] Media Sharing Networks
- [T0105.001] Photo Sharing
- [T0105.002] Video Sharing
- [T0106] Discussion Forums

[TA08] Conduct Pump Priming

- [T0042] Seed Kernel of Truth
- [T0045] Use Fake Experts

[TA09] Deliver Content

- [T0116] Comment or Reply on Content
- [T0116.001] Post Inauthentic Social Media Comment
- [T0117] Attract Traditional Media

[TA17] Maximize Exposure

- [T0039] Bait Influencer
- [T0049] Flood Information Space
- [T0049.007] Inauthentic Sites Amplify News and Narratives
- [T0118] Amplify Existing Narrative
- [T0119] Cross-Posting
- [T0119.002] Post across Platform

[TA11] Persist in the Information Environment

- [T0060] Continue to Amplify
- [T0128] Conceal Information Assets
- [T0128.001] Use Pseudonyms
- [T0128.004] Launder Information Assets
- [T0129] Conceal Operational Activity
- [T0129.006] Deny Involvement
- [T0129.007] Delete Accounts/Account Activity
- [T0129.009] Remove Post Origins



À PROPOS DE VIGINUM



Créé le 13 juillet 2021 et rattaché au SGDSN, le service de vigilance et de protection contre les ingérences numériques étrangères (VIGINUM) a pour raison d'être la protection du débat public numérique touchant aux intérêts fondamentaux de la Nation.

Ce service technique et opérationnel de l'État a pour mission de détecter et caractériser les campagnes de manipulation de l'information sur les plateformes numériques, impliquant des acteurs étrangers dans le but de nuire à la France et à ses intérêts.

Service de vigilance et protection contre les ingérences numériques étrangères | SGDSN

Crédit photo couverture : Photo de Carolin Thiergart sur Unsplash.